Vom Fachbereich für Mathematik und Informatik
der Technischen Universität Braunschweig
genehmigte Dissertation
zur Erlangung des Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
von

Dipl.-Inform. Andreas Fieger

Zuverlässige Datenkommunikation für mobile IP-basierte Systeme

1. Referentin:	Prof. Dr. M. Zitterbart, TU Braunschweig
2. Referent:	Prof. Dr. J. Eberspächer, TU München
Eingereicht am:	28.02.01
Mündliche Prüfung:	07.05.01

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Institut für Betriebssysteme und Rechnerverbund der Universität Braunschweig.

Mein besonderer Dank gilt Frau Prof. Dr. M. Zitterbart, die diese Arbeit betreut und ihre Durchführung an ihrem Lehrstuhl ermöglicht hat. Sie hat sowohl durch fachliche Ratschläge und intensive Diskussionen als auch durch ihre Unterstützung in organisatorischen Fragen ganz wesentlich zum Gelingen dieser Arbeit beigetragen. Für die Möglichkeit, die Ergebnisse der Arbeit zu veröffentlichen und auf Konferenzen zu präsentieren, sei ihr ebenfalls gedankt. Von ihrer Erfahrung bei dem Verfassen von wissenschaftlichen Veröffentlichungen und der Gestaltung von Konferenzvorträgen konnte ich enorm profitieren.

Für die Übernahme des Korreferats sei Herrn Prof. Dr. J. Eberspächer von der Technischen Universität München sehr herzlich gedankt.

Da die Arbeit zum Teil im Rahmen des von der DFG geförderten Projektes "Diensteintegrierendes Transportsystem für hybride Netzstrukturen" durchgeführt worden ist, gilt mein Dank auch der DFG für die Unterstützung des Forschungsprojektes.

Bedanken möchte ich mich auch bei meinen Kolleginnen und Kollegen des Instituts für Betriebssysteme und Rechnerverbund für die angenehme Zusammenarbeit, fruchtbare fachliche Diskussionen und gemeinsame Aktivitäten außerhalb des Arbeitsalltags. Ein besonderer Dank gilt meinem Kollegen J. Diederich, der sowohl – im Rahmen seiner Diplomarbeit – an der praktischen Umsetzung der Konzepte beteiligt war, als auch durch Anmerkungen zu Vorabversionen dieser Arbeit mitgeholfen hat, die Arbeit inhaltlich und in ihrer Form zu verbessern.

Außerdem sei an dieser Stelle den Studenten gedankt, die durch ihre Studienarbeiten, Diplomarbeiten und Hiwitätigkeiten einen Beitrag zur praktischen Umsetzung meiner Ideen und Konzepte geleistet haben. Zu erwähnen sind in diesem Zusammenhang die Herren A. Böger, J. Diederich, F. Haverkamp, W. Mader, S. Mhenni, A. Schoolmann und T. Ströhlein.

Nicht unerwähnt sollen die Personen bleiben, die mit ihren orthographischen Korrekturen einen Beitrag zu dieser Arbeit geleistet haben. Es sind dies Frau K. Keller und die Herren T. Fieger, S. Grutzeck, K. Krasnodembski und C. Toussaint. Auch ihnen gilt mein Dank.

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einleitung

Zwei wesentliche Entwicklungen prägen derzeit den Kommunikationssektor: Zum einen expandiert der Bereich der Mobilkommunikation sehr stark, zum anderen etabliert sich das Internet Protokoll (IP) über die Rechnerkommunikation hinausgehend zunehmend auch in anderen Bereichen der Kommunikation.

Die Anzahl der in letzter Zeit für die drahtlose Kommunikation entwickelten Systeme verdeutlicht die Dynamik in dem Bereich der Mobilkommunikation. Im Bereich drahtloser lokaler Netze sind IEEE 802.11 bzw. IEEE 802.11b Systeme standardisiert und werden inzwischen zunehmend installiert. Beispielsweise wird an deutschen Universitäten zur Zeit vermehrt zusätzlich zur drahtgebundenen Infrastruktur eine drahtlose Infrastruktur mittels drahtloser lokaler Netze aufgebaut. Auch bei Tagungen steht für Tagungsteilnehmer inzwischen häufig ein mittels drahtloser lokaler Netze realisierter Internetzugang zur Verfügung. Während drahtlose lokale Netze die Netzanbindung in einem größeren Bereich, z.B. einem Bürogebäude, ermöglichen, decken Bluetooth Systeme einen geringeren Entfernungbereich ab. Bluetooth Systeme sind für die drahtlose Kommunikation bis zu einer Entfernung von ca. 10 Metern geeignet und werden voraussichtlich ab Mitte 2001 im Handel verfügbar sein. Ein flächendeckender Datendienst mit akzeptablen Übertragungsraten wird durch den paketvermittelten Datendienst GPRS realisiert, der den schmalbandigen leitungsvermittelten Datendienst von GSM ablöst. UMTS als Mobilkommunikationssystem der nächsten Generation, mit dessen Aufbau im Laufe des Jahres 2001 begonnen wird, soll Datenraten von bis zu 2 Mbit/sec bereitstellen. Die genannten Systeme werden nebeneinander existieren, da sie sich hinsichtlich Flächenabdeckung und verfügbarer Bandbreiten ergänzen.

In der Vergangenheit war die Mobilkommunikation im wesentlichen von der Telefonie geprägt. Inzwischen erlangt aber auch die Datenkommunikation zunehmend an Bedeutung. In diesem Kontext muß der Zuverlässigkeit der Übertragung eine größere Beachtung geschenkt werden. Während bei der Sprachübertragung Übertragungsfehler in Grenzen toleriert werden können, trifft dies für Anwendungen, die auf eine zuverlässige Datenübertragung angewiesen sind, nicht zu. In Anbetracht der Tatsache, daß 85-95 Prozent des Internetverkehrs mittels des zuverlässigen Transportprotokolls TCP (Transmission Control Protocol) übertragen werden [TMW97], muß dem zuverlässigen Übertragungsdienst auch im Kontext der drahtlosen Anbindung mobiler Systeme besondere Aufmerksamkeit zuteil werden.

Das Internet Protokoll, das ursprünglich im Umfeld der Militärforschung entstanden ist und sich anschließend zu einem Standard für die Vernetzung von Geräten aus dem Bereich

der EDV entwickelt hat, erhält inzwischen zunehmend Einzug in Geräte des täglichen Lebens. Beispielsweise verwenden Persönliche Digitale Assistenten (PDA), auf der Voice-over-IP Technologie basierende Telefone und Geräte im Haushalt, wie z.B. Kühlschränke und Fernseher mit integriertem WWW-Browser oder Email-Client, das IP-Protokoll für die Anbindung an das Internet. Darüber hinaus ist davon auszugehen, daß auch im Sektor der Mobilkommunikation in den Endgeräten ein IP-Protokollstack realisiert sein wird. Die erforderliche Mobilitätsunterstützung kann mittels Mobile IP [Per98a] realisiert werden.

Die Ausführungen zeigen, daß die zuverlässige Datenkommunikation für mobile IP-basierte Endsysteme ein hochaktuelles Thema ist. Eine zentrale Frage ist, inwieweit die drahtlose Anbindung mittels eines der genannten Mobilkommunikationssysteme lediglich eine alternative Form der Anbindung zu z.B. Ethernet, Fast Ethernet, Token Ring, ISDN usw. darstellt, oder ob tiefgreifendere Auswirkungen die Folge sind. Diese Frage stellt sich insbesondere vor dem Hintergrund, daß temporäre Unterbrechungen des Übertragungskanals und Schwankungen der Bitfehlerwahrscheinlichkeit bzw. Burstfehlerwahrscheinlichkeit typisch für die funkbasierte Übertragung sind [ES98a], [AKL+95], [RSW98], bei der drahtgebundenen Übertragung in dieser Form aber nicht auftreten.

Inwieweit das Transportprotokoll TCP, das Ende-zu-Ende einen zuverlässigen Datendienst zur Verfügung stellt, mit der höheren Fehleranfälligkeit drahtloser Übertragungsstrecken zurechtkommt, wird in zahlreichen Veröffentlichungen betrachtet. Konsens herrscht hinsichtlich des negativen Einflusses der genannten Übertragungseigenschaften auf die Performance von TCP. Insbesondere die Ende-zu-Ende-Fehlerkorrektur und die Ende-zu-Ende-Lastkontrolle von TCP erweisen sich im Umfeld der fehleranfälligen, funkbasierten Übertragung als problematisch. Obwohl seit einigen Jahren weltweit an Forschungseinrichtungen intensiv an Lösungen gearbeitet wird und eine Vielzahl von Veröffentlichungen zu diesem Thema existieren, hat sich bis heute keine Lösung herauskristallisiert. Mit eine Ursache dafür ist die Tatsache, daß die Auswirkungen der fehleranfälligen Übertragung nicht vollständig lokal kompensiert werden können, sondern auch Ende-zu-Ende Auswirkungen haben. Manche der diskutierten Lösungsvorschläge adressieren nur einen Teil der auftretenden Probleme und unterscheiden sich dahingehend, welche Systeme für die jeweilige Lösung modifiziert werden müssen. Weiterhin ist ein Teil der Vorschläge nur schwer umsetzbar, da die erforderlichen Modifikationen an netzinternen Systemen des Internets nicht durchsetzbar sind. Eine praktikable Lösung muß diesen Aspekt mit berücksichtigen.

1.1 Problemstellung und Lösungsansatz

Da sich TCP als Ende-zu-Ende-Lösungsansatz als schlecht geeignet für die Realisierung eines zuverlässigen Datendienstes für drahtlos angeschlossene mobile Systeme erweist, sind alternative Ansätze erforderlich. Eine geeignete Lösung sollte sich sowohl nahtlos in das Internet integrieren lassen, als auch die verschiedenen im Kontext der funkbasierten Übertragung auftretenden Probleme – d.h. nicht nur einzelne Teilprobleme – adressieren. Die Anforderungen, die im Rahmen dieser Arbeit an eine geeignete Lösung gestellt werden, sind im folgenden aufgelistet:

- Keine Modifikation der TCP-Implementierung in den Festnetzrechnern
  Änderungen an dem Protokollstack – und dort insbesondere an der TCP-Implementie-

rung – aller Festnetzrechner, die potentielle Kommunikationspartner eines mobilen Systems sind, können nur schwer und in einem langwierigen Prozeß durchgesetzt werden. Aus diesem Grunde sollte ein Lösungsansatz ohne derartige Änderungen auskommen.

- Berücksichtigung von Unterbrechungen und höheren Bitfehlerraten
  Da temporäre Unterbrechungen des Übertragungskanals und höhere Bitfehlerraten typisch für die funkbasierte Übertragung sind, müssen diese berücksichtigt werden.

- Integration mit der Mobilitätsunterstützung im Internet auf Basis von Mobile IP
  Für die Mobilitätsunterstützung IP-basierter Endsysteme setzt sich im Internet zunehmend das Mobile IP Protokoll durch. Aus diesem Grunde sollte die Lösung mit Mobile IP zusammen einsetzbar sein.

In einem ersten Schritt werden in der vorliegenden Arbeit die in der Literatur vorgeschlagenen Lösungsansätze dahingehend analysiert, inwieweit sie die oben aufgeführten Anforderungen erfüllen können. Der *indirekte Transportansatz*, der zu Gruppe der proxy-basierten Ansätze gehört, erweist sich bei dieser Analyse als der am besten geeignete Lösungsansatz. Der wesentliche Vorteil des indirekten Ansatzes ist, daß er als einziger – ohne Änderung des TCP-Protokolls in Festnetzrechnern – auch im Falle längerer Unterbrechungen drastische, allenfalls im Falle signifikanter Netzwerküberlastungen angemessene, Lastreduktionen seitens der TCP-Instanzen vermeiden kann. Da sich vor dem Hintergrund der gestellten Anforderungen der indirekte Transportansatz, dessen grundlegendes Konzept in Abb. 1.1 dargestellt ist, als der Ansatz der Wahl herausstellt, sind die eigenen Arbeiten auf diesen Ansatz fokussiert.

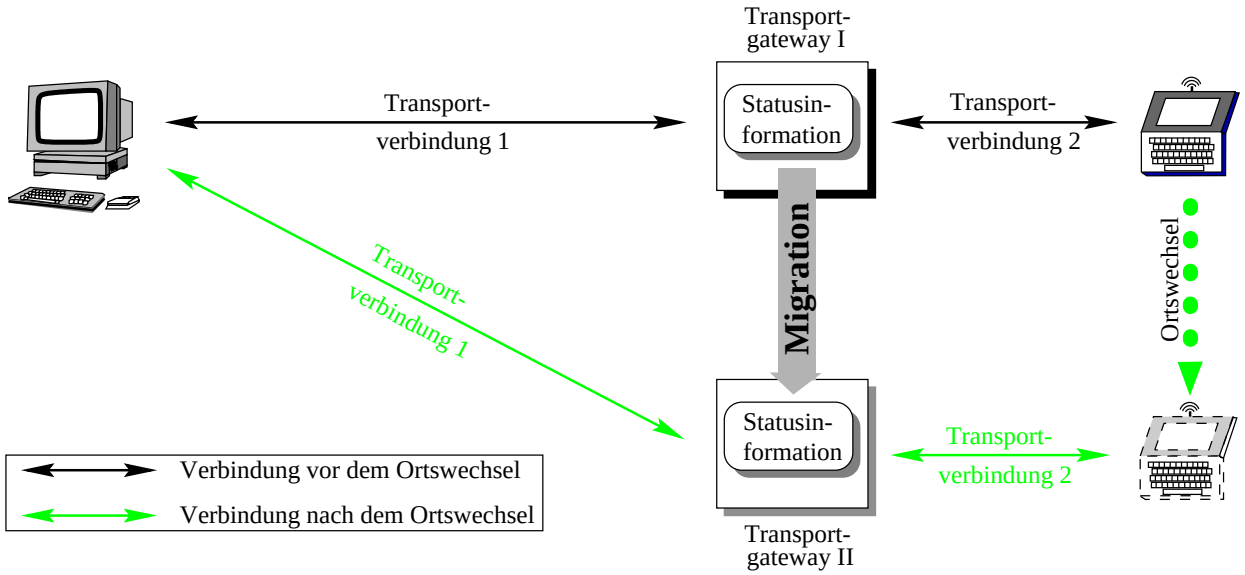


Abbildung 1.1: Grundkonzept des indirekten Transportansatzes

Beim indirekten Transportansatz wird eine ursprünglich Ende-zu-Ende operierende Transportverbindung in zwei Transportverbindungen unterteilt. Im sogenannten *Transportgateway* werden diese zwei Verbindungen gekoppelt. Für die Transportverbindung 1 wird das TCP-Protokoll eingesetzt. Somit ist die Interoperabilität zu TCP-basierten Festnetzrechnern sichergestellt. Für die Transportverbindung 2 können hingegen verschiedene, auf den jeweiligen Einsatzzweck zugeschnittene Protokolle verwendet werden. Beispielsweise kann ein Protokoll,

das für die Übertragung über eine GSM-Strecke optimiert ist [KRL+97], oder ein Protokoll, das sich durch einen minimierten Aufwand für die Protokollverarbeitung auf dem mobilen System auszeichnet [HA97], verwendet werden. Auch der Einsatz von TCP für die Transportverbindung 2 ist möglich [BB95b].

Während Ende-zu-Ende-Transportansätze ohne verbindungsspezifische Statusinformation in den Zwischensystemen auskommen, muß bei indirekten Transportansätzen die Statusinformation der Transportinstanzen im Transportgateway verwaltet werden. Da diese Statusinformation für den indirekten Transportansatz notwendig ist, muß auch im Fall der Mobilität von Endsystemen und der dadurch bedingten Routenänderungen die Statusinformation zu jedem Zeitpunkt im aktuell als Transportgateway fungierenden Zwischensystem verfügbar sein. Es ist die Aufgabe der sogenannten *Mobilitätsunterstützung für indirekte Transportansätze*, dies zu gewährleisten.

Ein zentrales Problem der in der Literatur beschriebenen indirekten Transportansätze ist, daß sie keine bzw. nur eine unzureichende Mobilitätsunterstützung bieten. Lediglich [BB95b] geht auf die Mobilitätsunterstützung für indirekte Transportansätze ein. Es wird das folgende Verfahren vorgeschlagen: Ändert sich auf Grund eines Ortswechsels eines mobilen Endsystems das Routing dahingehend, daß das Zwischensystem, das als Transportgateway fungiert, nicht mehr im Datenpfad liegt, so muß ein anderes Zwischensystem die Funktion des Transportgateways übernehmen (siehe Abb. 1.1). Damit dieses Zwischensystem als Transportgateway fungieren kann, muß zuvor eine *Migration der Statusinformation* zu diesem Zwischensystem erfolgen. Da in [BB95b] bei jedem Basisstationswechsel eine Migration vorgenommen werden muß und während der Migration der Statusinformation die Kommunikation in der Transportschicht für bis zu 1.4 Sekunden unterbrochen wird, muß diese Form der Mobilitätsunterstützung als unzureichend angesehen werden.

Das im Rahmen dieser Arbeit entwickelte OMIT-Konzept, das eine ***O**ptimierte **M**obilitätsunterstützung für **I**ndirekte **T**ransportansätze* bietet, setzt hier an und reduziert die durch die Mobilität bedingten Unterbrechungen signifikant. Es umfaßt

- das *Fast-Forwarding*-Konzept,
  eine Erweiterung des Mobile IP Protokolls, um die Anzahl der notwendigen Migrationen der Statusinformation zu reduzieren und

- das Konzept der *nebenläufigen Migration*,
  um im Falle einer Migration der Statusinformation die Dauer der Unterbrechung der Transportkommunikation zu verringern.

Bei den genannten Konzepten handelt es sich nicht um alternativ einzusetzende Konzepte, sondern um Konzepte, die im Zusammenspiel die optimierte Mobilitätsunterstützung realisieren. Aus diesem Grunde wird nicht nur der Nutzen jedes einzelnen Konzeptes für sich betrachtet, sondern werden auch Regeln für die Interaktion von Fast-Forwarding, Mobile IP und der nebenläufigen Migration in einem Transportgateway entwickelt.

Das OMIT-Konzept ist nicht auf einen bestimmten indirekten Transportansatz zugeschnitten, sondern ist für indirekte Transportansätze im allgemeinen geeignet. Es stellt somit ein Rahmenwerk für die Mobilitätsunterstützung indirekter Transportansätze dar. Es ist lediglich eine Mobilitätsunterstützung in der Netzwerkschicht auf Basis von Mobile IP vorauszusetzen, da das Fast-Forwarding-Konzept als Erweiterung von Mobile IP realisiert wird.

Im Rahmen einer prototypischen Implementierung der entworfenen Verfahren wird zum einen ihre Realisierbarkeit gezeigt, zum anderen der Nachweis erbracht, daß sich die durch die Mobilität der Endsysteme bedingten Unterbrechungen drastisch reduzieren lassen. Weitergehende Untersuchungen erfolgen auf simulativer Basis.

1.2 Gliederung der Arbeit

In Kapitel 2 werden die für das Verständnis der Arbeit erforderlichen Grundlagen beschrieben. Vor dem Hintergrund der verschiedenen Typen von Mobilität wird diskutiert, inwieweit eine Mobilitätsunterstützung in der Netzwerkschicht zwingend erforderlich ist. Die Grundlagen des Mobile IP Protokolls werden insoweit vorgestellt, wie sie für das Verständnis des Fast-Forwarding-Protokolls, einer Erweiterung von Mobile IP, erforderlich sind. Darüber hinaus werden die Protokollmechanismen von TCP beschrieben, die für die Performance-Einbußen von TCP im Umfeld der fehleranfälligen drahtlosen Übertragung verantwortlich sind. Das Kapitel umfaßt weiterhin eine Diskussion darüber, welche Auswirkungen die fehleranfällige drahtlose Kommunikation auf die Lastkontrolle von TCP hat. Es wird diskutiert, wie die Lastkontrolle von TCP auf einzelne bzw. mehrere aufeinanderfolgende Paketverluste reagiert und welche Durchsatzeinbußen die Folge sind.

Kapitel 3 klassifiziert und beschreibt die für die Problemlösung in der Literatur beschriebenen Ansätze. Darüber hinaus werden die Ansätze dahingehend bewertet, inwieweit sie die im Rahmen dieser Arbeit gestellten Anforderungen erfüllen können. Es wird begründet, warum die Klasse der indirekten Transportansätze als einzige den genannten Anforderungen gerecht werden kann. Die verschiedenen, in der Literatur beschriebenen indirekten Ansätze werden diskutiert und im Kontext der indirekten Ansätze auftretende ungelöste Probleme werden identifiziert. Als ein zentrales Problem erweisen sich die durch die Migration von Transportinstanzen bedingten Unterbrechungen. Mit eine Ursache für diese Unterbrechungen ist die Tatsache, daß bisher keine geeignete Mobilitätsunterstützung für mittels des indirekten Transportansatz angebundene mobile Endsysteme verfügbar ist.

In Kapitel 4 wird das in der vorliegenden Arbeit entwickelte Konzept für die ***O**ptimierte **M**obilitätsunterstützung für **I**ndirekte **T**ransportansätze* (OMIT) vorgestellt. Es werden Verfahren vorgeschlagen, wie die durch die Migration bedingten Unterbrechungen reduziert werden können. Es bieten sich zwei Ansätze an: Zum einen wird mittels des *Fast-Forwarding-Protokolls* die Zahl der notwendigen Migrationen reduziert. Die notwendigen Modifikationen und Erweiterungen an dem Mobile IP Protokoll werden im Detail beschrieben. Zum anderen kann das in diesem Kapitel vorgestellte Konzept der *nebenläufigen Migration* dazu eingesetzt werden, die durch die Migration bedingten Unterbrechungen bis auf 0.01 Sekunden zu reduzieren.

In Kapitel 5 wird untersucht, inwieweit die vorgeschlagenen Verfahren die Erwartungen erfüllen können. Die prototypische Implementierung und die Ergebnisse der Vermessung dieser Implementierung werden beschrieben. Die Ergebnisse der simulativen Untersuchungen sind ebenfalls Gegenstand der Betrachtungen in diesem Kapitel.

Kapitel 6 faßt die Arbeit und die Ergebnisse zusammen und liefert einen Ausblick auf weitere untersuchenswerte Aspekte im Kontext indirekter Transportansätze.

Kapitel 2

Grundlagen

In diesem Kapitel werden die für das Verständnis der Arbeit notwendigen Grundlagen beschrieben. Es wird auf die Grundlagen von Mobilkommunikationssystemen, das für die Internetanbindung mobiler IP-basierter Endsysteme eingesetzte Mobile IP Protokoll und auf das für die zuverlässige Übertragung im Internet verwendete Transportprotokoll TCP eingegangen.

Drahtlos angeschlossene Endgeräte können sich signifikant hinsichtlich ihrer technischen Leistungsfähigkeit unterscheiden. Darüber hinaus ist ein wesentliches Unterscheidungsmerkmal, inwieweit im Fall der Mobilität eines Endgerätes die Netzwerkverbindungen bereits gestarteter Anwendungen aufrechterhalten werden können. Neben diesen beiden Aspekten wird in Unterkapitel 2.1 auch auf verschiedene Strukturen von Mobilkommunikationssystemen eingegangen. Zusätzlich wird herausgearbeitet und anhand zahlreicher Literaturverweise untermauert, daß bei Mobilkommunikationssystemen auf Grund der Struktur der Kommunikationssysteme und der Übertragungseigenschaften der drahtlosen Übertragung signifikant häufiger temporäre Unterbrechungen und durch Bitfehler bedingte Paketverluste als bei der drahtgebundenen Übertragung auftreten.

Um trotz der Mobilität von IP-basierten Endgeräten zwischen verschiedenen Mobilkommunikationssystemen die Netzwerkverbindungen gestarteter Anwendungen aufrechterhalten zu können, ist eine Unterstützung in der Netzwerkschicht notwendig. Hierfür setzt sich im Internet das Mobile IP Protokoll zunehmend durch. Da außerdem das in in der vorliegenden Arbeit entwickelte Fast-Forwarding-Protokoll eine Erweiterung von Mobile IP darstellt und eine Integration des indirekten Transportansatzes mit Mobile IP erfolgt, ist ein grundlegendes Verständnis der Protokollmechanismen von Mobile IP notwendig. Sie werden in Unterkapitel 2.2 beschrieben.

Gegenstand der Betrachtungen in Unterkapitel 2.3 ist das Transportprotokoll TCP. Es wird sowohl auf die grundlegenden Protokollmechanismen eingegangen als auch ihr Verhalten im Kontext häufig auftretender Unterbrechungen und häufiger, durch Übertragungsfehler bedingter Paketverluste analysiert.

2.1 Mobilkommunikationssysteme

2.1.1 Endgeräte

Hinsichtlich der Größe, Leistungsfähigkeit und des Einsatzgebietes decken Geräte, deren Anbindung an das Festnetz drahtlos erfolgt, ein weites Einsatzspektrum ab. Sie unterscheiden sich sowohl hinsichtlich der Fähigkeiten der Endgeräte selbst als auch hinsichtlich der Bandbreiten und Technologien, die für die drahtlose Anbindung genutzt werden.

- Pager: Mit einem Pager können lediglich kurze Textnachrichten empfangen werden. Ein Versenden von Nachrichten ist nicht möglich. TCP/IP basierte Dienste stehen auf dem Pager nicht zur Verfügung. Abgesehen vom Pagerdienst sind keine weiteren Dienste auf dem Pager realisiert.

- Mobiltelefone: Das Mobiltelefon wurde ursprünglich lediglich als Endgerät für die Telefonie konzipiert. Inzwischen sind allerdings auch weitere Dienste für diese Endgeräte entwickelt worden, z.B. der Faxdienst und der SMS-Nachrichtendienst, der dem oben genannten Pagerdienst ähnelt, aber den bidirektionalen Nachrichtenaustausch ermöglicht. Der Funktionsumfang der Mobiltelefone wird zunehmend größer. Beispielsweise sind Terminkalenderfunktionen und Applikationen aus dem Unterhaltungsbereich inzwischen auf Mobiltelefonen realisiert. Während in der Vergangenheit das Mobiltelefon für über die Telefonie hinausgehende Dienste lediglich für die Anbindung von Laptops an das Internet eingesetzt wurde, werden inzwischen zunehmend Applikationen direkt auf dem Mobiltelefon realisiert. WAP-fähige Handys der neuesten Generation erlauben es dem Benutzer, ohne zusätzliche Hardware auf im Internet verfügbare Informationen zuzugreifen. Die Anbindung erfolgt allerdings nicht auf der IP-Ebene sondern über ein Gateway, d.h. das Mobiltelefon benötigt für die Kommunikation keine eigene IP-Adresse.

- Palmtop und Personal Digital Assistant (PDA): Hinsichtlich der Funktionalität ähnelt diese Gattung von Endgeräten eher Computern als den zuvor beschriebenen, um einige Funktionen erweiterten Mobiltelefonen. Auf PDAs lassen sich im Gegensatz zu Mobiltelefonen beispielsweise eigene Applikationen realisieren bzw. installieren. An Anwendungen sind im Funktionsumfang reduzierte Versionen von für Arbeitsplatzrechner entwickelten Programmen auch für PDAs verfügbar. Exemplarisch für diese Art von Geräten seien hier der Nokia Communicator und die Geräte der Palm-Serie des Herstellers 3COM genannt. Zur Netzanbindung wird diesen Geräten eine IP-Adresse zugewiesen, so daß sie aus dem Internet adressierbar sind.

- Laptop: Hinsichtlich der Rechenleistung unterscheiden sich Laptops heutzutage nicht mehr wesentlich von Arbeitsplatzrechnern. Anwendungen, die auf Arbeitsplatzrechnern verfügbar sind, können in der Regel auch auf Laptops eingesetzt werden. Die Internetanbindung erfolgt mittels einer eigenen IP-Adresse. Für die Funkanbindung werden in der Regel drahtlose LANs oder die ursprünglich für die Mobiltelefonie entwickelten Netze genutzt. Wesentliches Unterscheidungsmerkmal von den im nächsten Abschnitt beschriebenen Arbeitsplatzrechnern ist die Art der Stromversorgung und die Größe des Displays. Auf Grund der begrenzten Akkukapazitäten ist die Laufzeit von Laptops beschränkt und sind Maßnahmen zur Reduzierung des Energieverbrauches erforderlich. Während bei Arbeitsplatzrechnern Monitore mit einer Bildschirmdiagonale von 20 Zoll

oder mehr inzwischen zunehmend Verbreitung finden, sind die Displays von Laptops in der Regel nicht größer als 15 Zoll. Ursache hierfür sind allerdings nicht fertigungstechnische Randbedingungen von TFT-Displays, sondern die die Handlichkeit von Laptops bestimmende Baugröße dieser Geräte.

- Arbeitsplatzrechner: Arbeitsplatzrechner sind in der Regel drahtgebunden an das Internet angebunden. Allerdings sind auch Szenarien vorstellbar, in denen eine Netzanbindung über Funk sinnvoll ist. Beispielsweise läßt sich in Gebäuden, in denen sich wegen bautechnischer Restriktionen keine Netzwerkkabel neu verlegen lassen, erst durch den Einsatz drahtloser lokaler Netze ein Vernetzung realisieren. Auch in Katastrophenfällen, in denen nicht erst Zeit in den Aufbau einer drahtgebundenen Infrastruktur investiert werden kann, bietet es sich an, die Vernetzung mittels der Funktechnologie zu realisieren.

2.1.2 Netzanbindung nicht ortsgebundener Endsysteme

Prinzipiell muß bei räumlichen Positionsänderungen eines Endsystems unterschieden werden, ob durch die Positionsänderung eine Anpassung innerhalb des Kommunikationssystems notwendig wird oder nicht. Um Positionsänderungen, die Anpassungen im System erfordern, von solchen zu unterscheiden, die keine Anpassungen notwendig machen, wird der Begriff des *Ortswechsels* eingeführt. Eine Positionsänderung eines Endsystems ist genau dann ein Ortswechsel, wenn nach einer Positionsänderung Anpassungen im Kommunikationssystem erforderlich werden, da nicht mehr die gleichen Systeme durch Kommunikation auf der Schicht 2 erreicht werden können wie vor der Positionsänderung. Wird beispielsweise auf Grund einer Positionsänderung eines mobilen Endsystems ein Basisstationswechsel erforderlich, so handelt es sich um einen Ortswechsel. Wird hingegen auf Grund der Positionsänderung lediglich das Modulationsverfahren aber nicht die Basisstation gewechselt, so liegt kein Ortswechsel vor.

Aufgabe der sogenannten *Mobilitätsunterstützung* ist es, durch die entsprechende protokolltechnische Unterstützung dafür zu sorgen, daß das Endsystem auch nach einem Ortswechsel mit Kommunikationspartner im Internet Daten austauschen kann, d.h. die *Netzwerkkonnektivität* erhalten bleibt. Verfahren der Mobilitätsunterstützung gibt es in der Schicht 2, der Schicht 3 und im Kontext des in der vorliegenden Arbeit verfolgten indirekten Transportansatzes auch in der Schicht 4.

In Abhängigkeit davon, inwieweit eine Mobilitätsunterstützung realisiert ist, werden Endsysteme in die Gruppe der *stationären*, der *portablen* und der *mobilen* Endsysteme eingeteilt. Die Klassifikation des Grades der Mobilität der Endsysteme umfaßt zwei Dimensionen. Zum einen muß bei der Klassifikation berücksichtigt werden, inwieweit Größe und Gewicht eines Endsystems Mobilität überhaupt zulassen. Arbeitsplatzrechner lassen sich beispielsweise nur mit erhöhtem Aufwand an einen anderen Ort transportieren. Zum anderen muß die protokolltechnische Unterstützung der Ortswechsel von drahtlos angeschlossenen Endsystemen mit in Betracht gezogen werden.

Als Klassifikationskriterium dient im folgenden die im Endsystem realisierte protokolltechnische Unterstützung, um nach einem Ortswechsel die Netzwerkkonnektivität wiederherzustellen. Ein Typ von Endgerät, z.B. ein Laptop oder ein PDA, ist nicht unbedingt genau einer Gruppe zugeordnet. In Abhängigkeit davon, welche protokolltechnische Mobilitätsunterstützung der Laptop bzw. PDA nutzt, erfolgt die Einordnung entweder in die Gruppe der stationären, portablen oder mobilen Endsysteme.

- Stationäre Endsysteme: Bei stationären Endsystemen sind keine Mechanismen für die Mobilitätsunterstützung realisiert. Die Netzwerkinterfaces stationärer Endsysteme werden manuell konfiguriert. Diese Systeme sind nicht dafür ausgelegt, häufig an verschiedenen Orten betrieben zu werden. Im Falle eines Ortswechsels – beispielsweise nach dem Umzug eines drahtlos oder drahtgebunden angeschlossenen stationären Endsystems in eine andere Abteilung – muß die Netzwerkverbindung von Hand rekonfiguriert werden. Weiterhin müssen alle das Netzwerk benutzenden Anwendungen neu gestartet werden. Die Rekonfiguration von Hand macht die Anbindung eines stationären Endsystems an einem anderen Ort mühsam und arbeitsaufwendig. Bei sogenannten portablen Endsystemen, die im folgenden beschrieben werden, ist eine Rekonfiguration von Hand nicht erforderlich.

- Portable Endsysteme: Wesentliches Merkmal portabler Systeme ist, daß nach einem Ortswechsel die Netzwerkkonnektivität automatisiert unter der Kontrolle eines geeigneten Protokolls wiederhergestellt wird. Für IP-basierte Systeme kann hierfür das Dynamic Host Configuration Protocol (*DHCP*) [Dro97], [PJ95], [Per98a] eingesetzt werden. Dieses Protokoll nutzt einen serverbasierten Ansatz, bei dem ein sogenannter DHCP-Server das portable System nach einem Ortswechsel mit den nötigen Konfigurationsdaten für das Netzwerkinterface versorgt. Trotz der automatischen Konfiguration ist der Ortswechsel für die Anwendungen nicht transparent. Da sich die IP-Adresse des portablen Systems bei einem Ortswechsel ggf. ändert, können Netzwerkverbindungen nach der Rekonfiguration nicht weiter genutzt werden. Anwendungen, die diese Netzwerkverbindung nutzen, müssen beendet und neu gestartet werden. Bei Endgeräten, die das Windows 95/98 Betriebssystem nutzen, ist sogar ein Neustart des Endgerätes notwendig, da das Netzwerkinterface lediglich beim Booten konfiguriert werden kann. Der Einsatz portabler Endgeräte an verschiedenen Orten – mit der Restriktion des Neustartes der Anwendungen – wird als *Nomadic Computing* bezeichnet.

- Mobile Endsysteme: Bei Ortswechseln dieses Typs von Endgeräten wird wie bei den portablen Systemen die Rekonfiguration automatisch vorgenommen. Darüber hinaus entfällt auch die Notwendigkeit eines Neustartes des Endgerätes bzw. der Anwendungen nach einem Ortswechsel. Der Einsatz mobiler Endgeräte an verschiedenen Orten ohne die Notwendigkeit eines Neustartes der Anwendungen nach einem Ortswechsel wird als *Mobile Computing* bezeichnet. Innerhalb eines einzelnen Mobilkommunikationsnetzes, z.B. GSM, kann die Unterstützung mobiler Endsysteme mittels der in diesem Mobilkommunikationsnetz realisierten Mobilitätsunterstützung erfolgen. Eine netzübergreifende Mobilitätsunterstützung für IP-basierte Systeme erfordert hingegen andere Verfahren. In [SB00] wird eine Erweiterung von TCP skizziert, die es erlaubt, die IP-Adressen der Verbindungsendpunkte etablierter TCP-Verbindungen zu modifizieren und somit den Neustart von Anwendungen nach Ortswechseln zu vermeiden. Während es sich beim genannten Verfahren lediglich um einen Lösungsansatz handelt, setzt sich das von der IETF entwickelte Mobile IP Protokoll zunehmend für die Mobilitätsunterstützung IP-basierter mobiler Endsysteme durch. Auf das Mobile IP Protokoll wird im Detail in Kapitel 2.2 eingegangen.

Abb. 2.1 zeigt eine Einordnung der verschiedenen in Kapitel 2.1.1 beschriebenen Typen von Endgeräten und ihre Zuordnung zur Gruppe der stationären, portablen bzw. mobilen Endgeräte. Am Beispiel des Laptops ist klar zu erkennen, daß manche Endgeräte prinzipiell

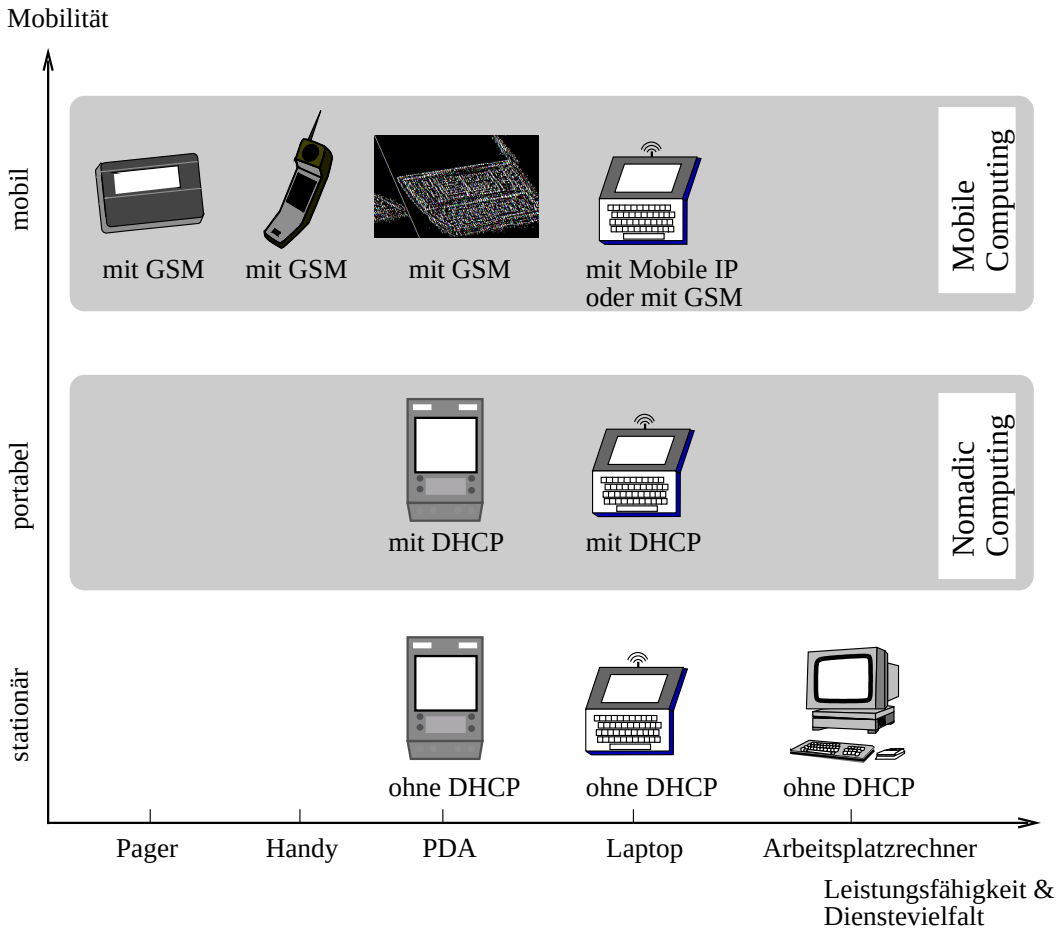


Abbildung 2.1: Klassifikation von Endgeräten

stationär, portabel oder mobil betrieben werden können. Für die Zuordnung zu einer der aufgeführten Gruppen ist entscheidend, welche protokolltechnische Mobilitätsunterstützung zum Einsatz kommt. Ein Laptop kann stationär, bei Einsatz des Protokolls DHCP portabel und unter Verwendung des Mobile IP Protokolls mobil eingesetzt werden. Erfolgt die Netzanbindung mittels GSM, kann anstatt der Mobilitätsunterstützung durch Mobile IP auch die intern in GSM realisierte Mobilitätsunterstützung eingesetzt werden.

Die Zuordnung eines PDAs zu einer der drei Gruppen ist vom Typ des PDAs abhängig. Ein Palmtop von 3COM kann beispielsweise mit oder ohne DHCP betrieben werden. Es ist allerdings weder eine Mobilitätsunterstützung durch GSM noch mittels Mobile IP verfügbar. Daraus ergibt sich die Einordnung in die Gruppe der stationären bzw. portablen Endgeräte. Der Nokia Communicator hingegen ist der Gruppe der mobil einsetzbaren Endgeräte zuzurechnen. Allerdings nutzt dieses Endgerät nicht Mobile IP für die protokolltechnische Unterstützung der Mobilität, sondern die in GSM intern realisierte Mobilitätsunterstützung.

Mobiltelefone und Pager sind der Gruppe der für den mobilen Einsatz konzipierten Geräte zuzuordnen. Portable Varianten dieser Geräte gab es lediglich in Mobilkommunikationssystemen der ersten Generationen, als noch keine Mobilitätsunterstützung verfügbar war.

2.1.3 Struktur drahtloser Kommunikationssysteme

Hinsichtlich der Struktur drahtloser Kommunikationssysteme lassen sich zwei Typen unterscheiden: Sogenannte *Ad-Hoc-Netzwerke*, die ohne drahtgebundene Infrastruktur operieren können, und sogenannte *Infrastrukturnetzwerke*, die zusätzlich zur drahtlosen Übertragungstechnik auch eine drahtgebundene Infrastruktur nutzen. Die beiden genannten Typen von Kommunikationssystemen unterscheiden sich hinsichtlich der Ausdehnung des räumlichen Bereiches, in dem die drahtlose Kommunikation möglich ist.

2.1.3.1 Ad-Hoc-Netzwerke

Es ist das Konzept von Ad-Hoc-Netzwerken, ohne zusätzliche Konfigurationsarbeiten und ohne zusätzliche Infrastruktur drahtlose Kommunikation zwischen den Systemen zu ermöglichen, die das Ad-Hoc-Netzwerk bilden. Bluetooth Systeme [HNI+98] und IEEE 802.11 Systeme [IEE99] im Ad-Hoc-Modus bieten diese Funktionalität. Die Systeme innerhalb eines Ad-Hoc-Netzwerkes können direkt untereinander kommunizieren. Kommunikation zu im Internet lokalisierten Systemen ist nur möglich, falls eines der Systeme des Ad-Hoc-Netzwerkes auch über einen Internetzugang verfügt.

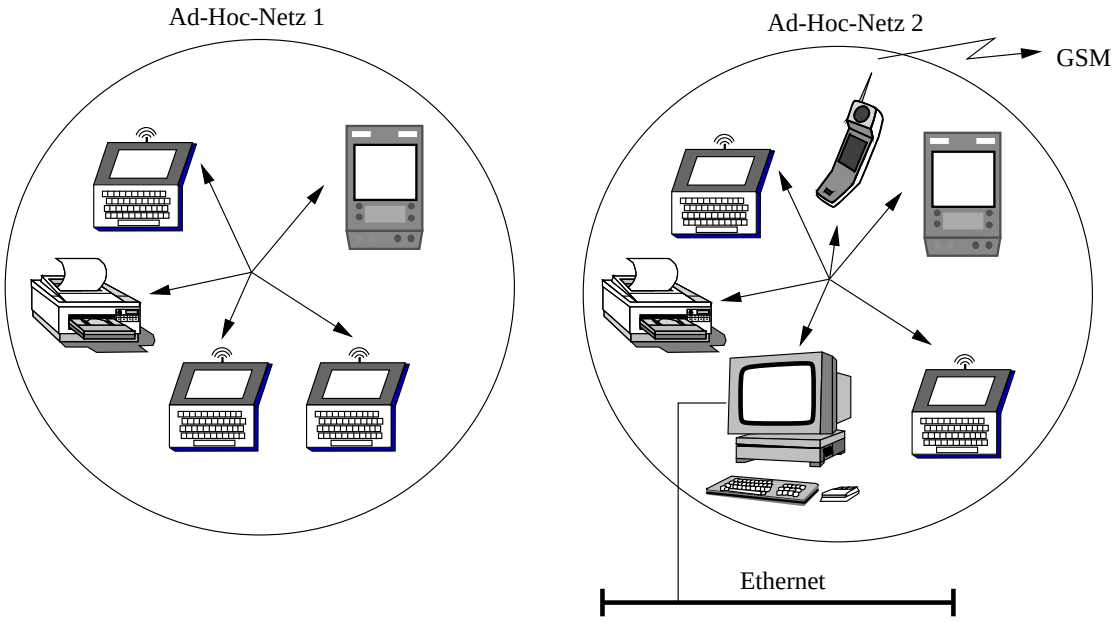


Abbildung 2.2: Ad-Hoc-Netzwerke

In Abb. 2.2 sind zwei voneinander unabhängige Ad-Hoc-Netzwerke dargestellt. Die in Netz 1 dargestellte Situation ergibt sich zum Beispiel, falls mehrere Personen in einem Besprechungsraum ihre Laptops bzw. PDAs nutzen und auch untereinander kommunizieren wollen. Der im Besprechungsraum fest installierte Drucker ist ebenfalls in das Ad-Hoc-Netzwerk eingebunden und kann von jedem der Laptops direkt mittels drahtloser Kommunikation genutzt werden. Da keines der Endsysteme zusätzlich zu seiner Einbindung in das Ad-Hoc-Netzwerk eine Anbindung an das Internet hat, ist der Datenaustausch auf die Kommunikation innerhalb des Ad-Hoc-Netzwerkes beschränkt. Kommunikation mit Endsystemen des Netzes 2 ist nicht möglich. Es handelt sich somit um eine Kommunikationsinsel.

Im Netz 2 in Abb. 2.2 sind in das Ad-Hoc-Netzwerk Geräte eingebunden, die an das Festnetz angebunden sind. Zusätzlich zu dem Drucker ist ein PC in dem Besprechungsraum fest installiert, der seinerseits über Ethernet an das Internet angebunden ist. Da der PC auch in das Ad-Hoc-Netzwerk eingebunden ist, ergibt sich auch für die anderen Systeme des Ad-Hoc-Netzwerkes die Möglichkeit des Internetzuganges. Darüber hinaus könnte der Internetzugang im skizzierten Beispiel auch drahtlos über das Mobiltelefon erfolgen.

2.1.3.2 Multi-Hop-Netzwerke

Die räumliche Ausdehnung von Ad-Hoc-Netzwerken läßt sich vergrößern, falls die das Ad-Hoc-Netzwerk bildenden Endsysteme zusätzlich über eine sogenannte *Forwarding*-Funktionalität verfügen. In Abb. 2.3 können der PDA und der PC auf Grund der räumlichen Distanz nicht direkt miteinander kommunizieren. Unter der Annahme, daß Laptop A und Laptop B Pakete weiterleiten können, ist dennoch eine Kommunikation zwischen dem PDA und dem PC möglich. Die Forwarding-Fähigkeit der einzelnen mobilen Endsysteme ermöglicht es, sogenannte *Multi-Hop-Netzwerke* aufzubauen und den räumlichen Bereich, in dem die drahtlose Kommunikation möglich ist, zu vergrößern.

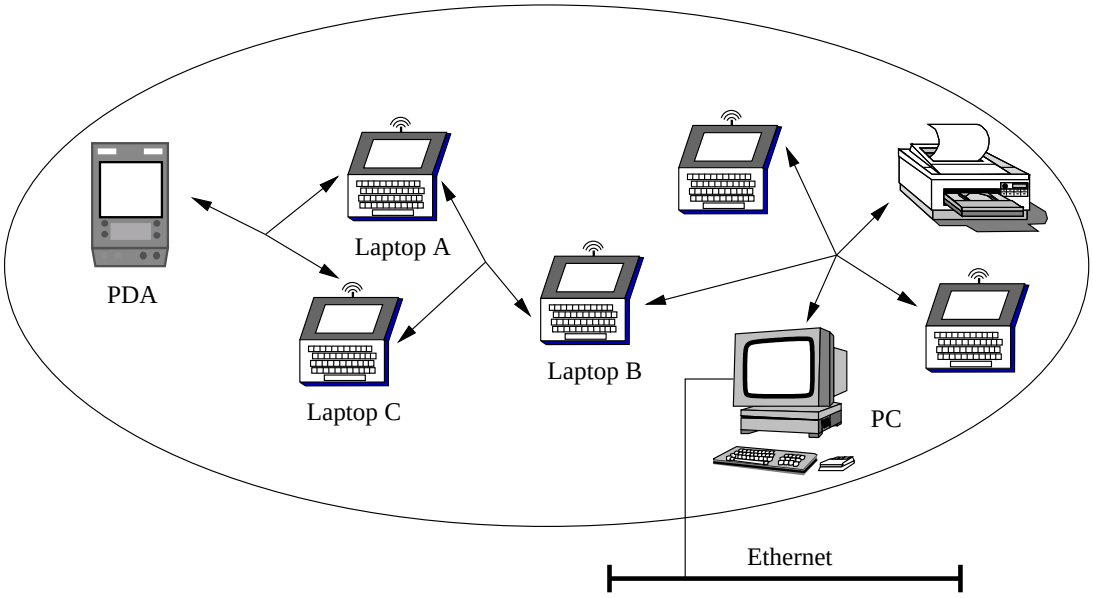


Abbildung 2.3: Multi-Hop-Netzwerk

In Multi-Hop-Netzwerken muß dem Routing [RT99] besondere Aufmerksamkeit zuteil werden. Da die Endsysteme, die das Forwarding übernehmen, nicht notwendigerweise stationär sind, ändern sich ggf. die Routingwege. Entfernt sich im in Abb. 2.3 skizzierten Szenario Laptop A vom PDA und von Laptop B, so kann er für den PDA nicht mehr die Pakete zu Laptop B weiterleiten. Sobald das Routing entsprechend angepaßt wurde, könnte im dargestellten Szenario Laptop C das Forwarding übernehmen. Auf Grund der Dynamik und der Notwendigkeit einer häufigen Anpassung des Routings in großen, viele Systeme umfassenden Multi-Hop-Netzwerken ist das Routing problematisch. Es ist nicht sichergestellt, daß jedes mobile Endsystem zu jedem Zeitpunkt auch erreichbar ist. Aus diesem Grund haben Multi-Hop-Netzwerke mit mobilen, für das Forwarding verantwortlichen Systemen im Vergleich zu

Netzwerken mit weitgehend statischen Netztopologien höhere Paketverlustraten und häufigere temporäre Unterbrechungen zur Folge. In [DPR00], [BMJ+98] beschriebene simulative Untersuchungen, die Paketverlustraten von bis zu 50 Prozent ergeben, bestätigen dies.

2.1.3.3 Infrastrukturnetzwerke

Um die geographische Ausdehnung des Bereiches, in dem die drahtlose Kommunikation möglich ist, zu vergrößern, können entweder Multi-Hop-Netzwerke oder sogenannte Infrastrukturnetzwerke eingesetzt werden. Während bei Multi-Hop-Netzwerken eine größere Ausdehnung durch mobile Systeme mit Forwarding-Fähigkeit ermöglicht wird, ist eine derartige Unterstützung seitens der mobilen Systeme bei Infrastrukturnetzwerken nicht erforderlich. Drahtlose lokale Netze gemäß des IEEE 802.11 Standards [IEE99], das GSM-Netz [EV97] und das UMTS-Netz [HWB00] sind Beispiele für Systeme, die als Infrastrukturnetzwerke konzipiert sind.

Um eine Netzabdeckung zu erzielen, die über die Reichweite eines Senders hinausgeht und unter Umständen sogar flächendeckend ist, wird die vom drahtlosen Netzwerk abzudeckende Fläche in mehrere *Funkzellen* unterteilt. Für jede dieser Zellen übernimmt ein ausgewiesenes System die funktechnische Versorgung. Dieses ausgewiesene System wird als *Basisstation* oder *Access Point* bezeichnet. Insbesondere für drahtlose lokale Netze ist der Begriff Access Point gebräuchlich. Die Kopplung der Basisstationen erfolgt über das Kommunikationssystem. Abb. 2.4 zeigt die grundlegende Architektur von Infrastrukturnetzwerken mit den wesentlichen Komponenten. Über das Gateway kann eine Anbindung an andere Netze erfolgen.

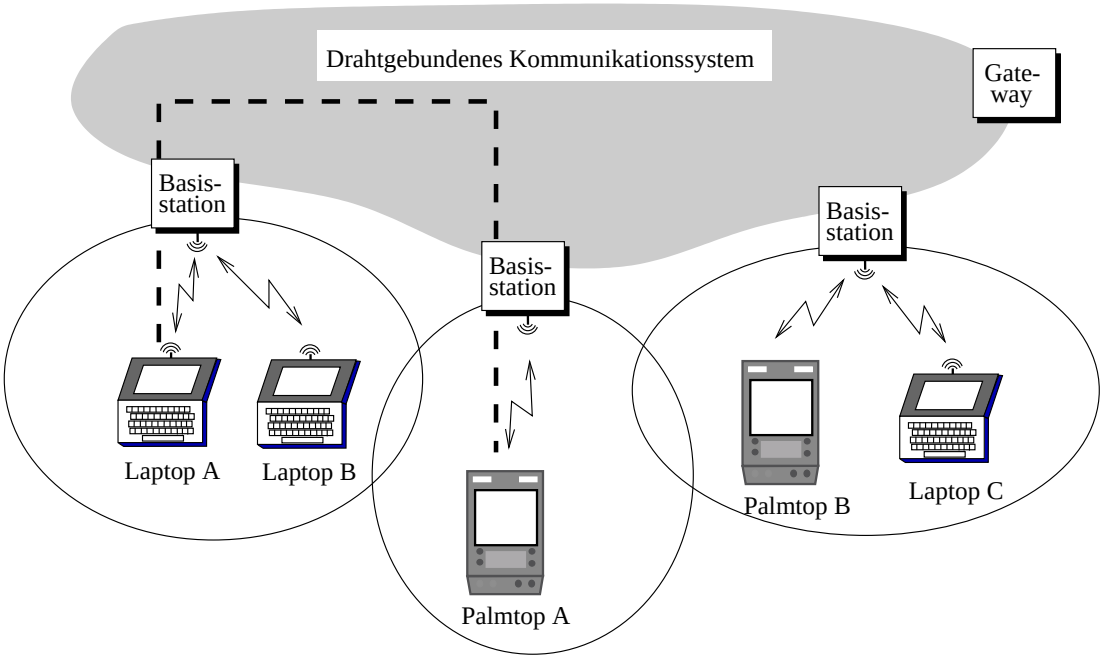


Abbildung 2.4: Architektur eines Infrastrukturnetzwerkes

Zwei Endsysteme, die sich aktuell in der gleichen Zelle aufhalten, kommunizieren nicht direkt miteinander, obwohl dies hinsichtlich der Reichweite der Funksignale unter Umständen möglich wäre. Stattdessen werden die Pakete zunächst an die Basisstation gesandt und von dieser anschließend zum mobilen Empfänger in der gleichen Zelle. Befinden sich sendendes

und empfangendes Endsystem in zwei verschiedenen Zellen, werden die Pakete zunächst zur Basisstation der Zelle des Senders übertragen. Von dort werden sie über das Kommunikationssystem zu der Basisstation weitergeleitet, über die der Empfänger angebunden ist. Diese Basisstation liefert die Pakete an das empfangende Endsystem aus.

Eine Basisstation kann nur solange die Funkanbindung eines mobilen Systems übernehmen, wie sich das mobile System in der zugehörigen Funkzelle aufhält. Wechselt das mobile System in eine andere Funkzelle, muß die dortige Basisstation die Funkanbindung übernehmen. Es wird ein sogenannter *Basisstationswechsel* erforderlich. Die hierfür notwendigen Verfahren sind in der Schicht 2 des Protokollstacks realisiert. Sie umfassen unter anderem die Abmeldung des mobilen Systems bei der alten Basisstation und die Anmeldung bei der neuen Basisstation.

Analoge und digitale terrestrische Rundfunksysteme, terrestrische Mobilkommunikationssysteme für die Daten- bzw. Sprachkommunikation und drahtlose lokale Netze sind als Infrastrukturnetzwerke konzipiert. Sie unterscheiden sich allerdings hinsichtlich der im folgenden aufgelisteten Kriterien:

- Richtung des Nutzdatentransportes: Prinzipiell muß unterschieden werden, ob Nutzdaten nur unidirektional zum drahtlos angeschlossenen Endsystem gesendet werden können oder aber bidirektionale Kommunikation möglich ist.
- Art der Nutzdaten: Audio, Video bzw. Daten
- Zellengröße: Von der Zellengröße hängt unmittelbar die Anzahl der für eine vollständige Versorgung notwendigen Basisstationen ab. Darüber hinaus hat die Zellengröße auch Einfluß auf die erforderliche Sendeleistung und die Anzahl der unterstützbaren Endsysteme.
- Netzabdeckung
- verfügbare maximale Datenrate
- Notwendigkeit der Mobilitätsunterstützung

Terrestrische Rundfunksysteme
Terrestrische Rundfunksysteme sind als Broadcastsysteme ausgelegt. Analoge Systeme verfügen über keinen Rückkanal, d.h. sie sind lediglich für die unidirektionale Kommunikation konzipiert. Digital Audio Broadcast (DAB) bzw. Digital Video Broadcast (DVB) kann terrestrisch, über Satellit oder über Kabel verbreitet werden. Die terrestrische Variante nutzt als Rückkanal eine Modemverbindung, d.h. die Kommunikation über den Rückkanal erfolgt nicht über das terrestrische Rundfunksystem. Bestehende analoge Systeme transportieren Audio und Video zu den Endsystemen. Zukünftige Digital Audio Broadcast bzw. Digital Video Broadcast Systeme unterstützen hingegen auch die Übertragung multimedialer Daten. Da es sich bei diesen terrestrischen Systemen um Broadcastsysteme handelt, muß nicht entschieden werden, in welche Zellen Daten ausgestrahlt werden. Aus diesem Grund ist keine Mobilitätsunterstützung notwendig. Wegen der Beschränkung der funkbasierten Übertragung auf die unidirektionale Kommunikation und mangels der Möglichkeit, mobile Endsysteme individuell zu adressieren, sind terrestrische Rundfunksysteme nur schlecht für die Internetanbindung mobiler Endsysteme geeignet. Sie werden wegen dieser Beschränkung im Rahmen der vorliegenden Arbeit nicht weiter betrachtet.

Terrestrische Mobilkommunikationssysteme
Die Entwicklung flächendeckender terrestrischer Mobilkommunikationssysteme wurde in der Vergangenheit wesentlich von dem Ziel eines Telefondienstes für mobile Teilnehmer getrieben. Systeme der ersten Generation wurden mittels analoger Technologien realisiert. Das A-Netz ab 1958, das B-Netz ab 1972 und das C-Netz in Deutschland, das Nordic Mobile Telephone Netz (NMT) ab 1981 in Skandinavien und das Advance Mobile Phone System (AMPS) ab 1983 in den USA und Kanada sind analoge Systeme der ersten Generation. Diese Auflistung zeigt bereits, daß sich kein weltweiter Standard entwickeln konnte, sondern mehrere zueinander inkompatible Systeme zeitgleich nebeneinander existierten.

In Systemen der zweiten Generation erfolgte sowohl die Sprachübertragung als auch die Signalisierung digital. Wie auch bei den Systemen der ersten Generation entwickelten sich weltweit mehrere zueinander nicht kompatible Standards. In den USA entstanden die digitalen IS-95 und IS-136 Systeme. Die europäischen Staaten einigten sich auf das digitale Global System for Mobile Communication (GSM) [EV97], [MP92], das im Jahre 1991 standardisiert wurde. Dieses System ermöglicht Roaming zwischen verschiedenen Providern und zwischen Ländern, in denen das GSM System installiert ist. Mit Installationen in über 130 Ländern im Jahre 1999 ist es das derzeit am weitesten verbreitete System.

Mobilkommunikationssysteme auf der Basis von GSM unterstützen sowohl die Kommunikation zum mobilen Endsystem, als auch Kommunikation, bei der das mobile System die Datenquelle darstellt. Auch die Kommunikation zwischen zwei mobilen Systemen ist möglich. Desweiteren ist die Kommunikation nicht auf einen reinen Audio-Dienst beschränkt. Es ist zusätzlich ein Nachrichtendienst, ein Faxdienst und ein Dienst zur Übertragung beliebiger Daten nutzbar. Da das Netz ursprünglich für die Telefonie entwickelt wurde, wurde es mittels des leitungsorientierten Kommunikationsparadigmas realisiert. Somit war es naheliegend, auch für den Datendienst den leitungsorientierten Ansatz zu nutzen. Andernfalls wären massive Änderungen in dem Kommunikationssystem, das die Basisstationen verbindet, notwendig geworden.

In GSM werden Übertragungsraten von 9.6 Kbit/sec [EV97] (ohne Kanalbündelung) bzw. mittels HSCSD [ETS97] von bis zu 57.6 KBit/sec (mit Kanalbündelung) erreicht. Der General Packet Radio Service (GPRS) [BW97], eine Erweiterung von GSM, nutzt das paketvermittelte Kommunikationsparadigma und bietet im Endausbau Datenraten bis zu 150 Kbit/sec. Dieser Dienst steht seit Anfang 2001 – allerdings mit einer maximalen Übertragungsrate von 53.6 Kbit/sec – zur Verfügung. UMTS [HWB00] als Mobilkommunikationssystem der nächsten Generation soll flächendeckend Datenraten von 384 Kbit/sec und im lokalen Bereich von bis zu 2 Mbit/sec bereitstellen.

Anstatt flächendeckend einen Datendienst mit den oben genannten – im Vergleich zum Festnetz – geringen Bandbreiten zu realisieren, können auch Infrastrukturnetzwerke aufgebaut werden, die zwar keine weitgehend vollständige Flächenabdeckung bieten, dafür aber in dem Bereich, den sie abdecken, deutlich höhere Datenraten zur Verfügung stellen. Die im nächsten Abschnitt beschriebenen drahtlosen lokalen Netze bieten drahtlos angeschlossenen Endsystemen deutlich höhere Datenraten als die flächendeckenden terrestrischen Systeme.

Drahtlose lokale Netze
Drahtlose lokale Netze [Wav96], [IEE99] sind ebenfalls als Infrastrukturnetzwerke ausgelegt. Wie der Name schon sagt, sind diese Netze nur für eine lokale, örtlich begrenzte Flächenab-

deckung konzipiert. Der Ausdehnungsbereich ähnelt dem drahtgebundener lokaler Netze. Beispielsweise kann mittels drahtloser lokaler Netze die Netzwerkkonnektivität einzelner Abteilungen oder eines ganzen Firmenareals realisiert werden. Je nach verwendeter Technologie liegt die Reichweite einer Basisstation in der Größenordnung von ca. 20 bis ca. 200 Metern. Von wesentlicher Bedeutung ist hierbei, ob die Kommunikation innerhalb oder außerhalb von Gebäuden erfolgt. Eine Basisstation, die in einem Gebäude lediglich eine Zelle mit einem Radius von ca. 50 Metern versorgt, kann in baugleicher Ausführung und mit gleicher Sendeleistung außerhalb eines Gebäudes einer deutlich größeren Zelle – in der Größenordnung von mehreren 100 Metern – eine ausreichende Funkversorgung bieten.

Drahtlose lokale Netze sind sowohl für den Telefondienst als auch für den Datendienst entwickelt worden. Die für den Telefondienst ausgelegten Netze sind als leitungsvermittelte Netze, die für den Datendienst konzipierten Netze als paketvermittelte Netze realisiert. In beiden Netzen ist eine Mobilitätsunterstützung notwendig, um Daten- bzw. Sprachverbindungen trotz der unter Umständen notwendigen Basisstationswechsel mobiler Endsysteme aufrechterhalten zu können.

2.1.3.4 Überblick über drahtlose Netze

Tabelle 2.1 zeigt eine Auflistung verschiedener drahtloser Kommunikationstechnologien. In Abhängigkeit von der Größe des Abdeckungsbereiches erfolgt die Einordnung in die Klasse 'short range', 'wireless LAN' (W-LAN) oder 'wireless wide area network' (W-WAN). In die letzte Gruppe werden drahtlose Netze eingeordnet, die flächendeckend Netzanbindung bieten. Zusätzlich zu dieser Einordnung kann der Tabelle entnommen werden, welche Datenraten von den Netzen zur Verfügung gestellt werden und ob sie als Infrastrukturnetzwerke ausgelegt sind oder auch als Ad-Hoc-Netzwerke einsetzbar sind. Einige der aufgeführten Systeme unterstützen mehrere verschiedene Datenraten.

	System	Datenrate	Infrastruktur-netzwerk	Ad-Hoc-Netzwerk
short range	IrDA	155 Kbit/sec, 4 Mbit/sec	-	x
	Bluetooth [HNI+98]	721 Kbit/sec	-	x
W-LAN	ARLAN [ARL97]	1/2 Mbit/sec	x	-
	WaveLAN [Wav96]	1/2 Mbit/sec	x	-
	IEEE 802.11 [IEE99]	2/11 Mbit/sec	x	x
W-WAN	GSM [EV97]	9.6 Kbit/sec	x	-
	HSCSD [ETS97]	57.6 Kbit/sec	x	-
	GPRS [BW97]	150 Kbit/sec	x	-
	UMTS [HWB00]	384 Kbit/sec	x	-

Tabelle 2.1: Aufstellung drahtloser Netze

2.1.4 Grundlegende Probleme der Mobilkommunikation

Bedingt durch die Struktur und die Übertragungseigenschaften drahtloser Netze sind für den erfolgreichen Aufbau und Einsatz dieser Netze eine Reihe von zusätzlichen Randbedingungen

zu berücksichtigen, die es in dieser Form bei der drahtgebundenen Kommunikation bisher nicht gab. Darüber hinaus ergeben sich wegen der erforderlichen Handlichkeit der mobilen Endgeräte und der begrenzten Akkukapazitäten für ihre Energieversorgung weitere Anforderungen. Im folgenden sind zu lösende Probleme aufgelistet:

- Medienzugriff
  Da ggf. mehrere mobile Systeme gemeinsam denselben Funkkanal nutzen, ist eine geeignete Medienzugriffskontrolle erforderlich. Diese muß auch dann funktionieren, wenn nicht alle mobilen Systeme die Funksignale aller anderen, den gemeinsamen Funkkanal nutzenden Systeme empfangen können.

- Unterstützung von Basisstationswechseln und Lokalisierung mobiler Systeme
  Bedingt durch die Mobilität ist nach einem Ortswechsel eines mobilen Systems ggf. die Kommunikation mit der bisherigen Basisstation nicht mehr möglich. Die Unterstützung von Basisstationswechseln sorgt dafür, daß trotz der Mobilität von Endsystemen deren funktechnische Anbindung gewährleistet ist. Darüber hinaus müssen mobile Systeme, unabhängig davon welche Basisstation sie für die Kommunikation nutzen, zuverlässig lokalisiert werden können.

- Sicherheit
  Im Gegensatz zur drahtgebundenen Kommunikation ist sowohl für das Mitlauschen von Daten als auch für die Integration eines mobilen Systems in ein drahtloses Netz keine Ankopplung an ein Kabel erforderlich. Sicherheitsmechanismen zur Authentifizierung und Verschlüsselung sind deshalb zusätzlich notwendig, um Schutz vor feindlichen Angriffen zu gewährleisten.

- Stromverbrauch
  Aufgrund begrenzter Akkukapazitäten sollte der für die Kommunikation erforderliche Anteil der Akkukapazität möglichst gering gehalten werden.

Die bisher genannten Probleme werden in dieser Arbeit nicht weiter ausgeführt. Für sie sind bereits eine Vielzahl von Lösungsansätzen entwickelt worden. In verfügbaren und existierenden drahtlosen Netzen kommen diese bereits teilweise zum Einsatz. Lösungsansätze für die im folgenden aufgelisteten Probleme werden hingegen noch kontrovers diskutiert und sind ein zentraler Bestandteil dieser Arbeit:

- Unterbrechungen der Kommunikation auf dem Funkkanal,
- zeitweilig höhere Bitfehlerraten des Funkkanals und
- schwankende Übertragungseigenschaften.

Übertragungseigenschaften der drahtlosen Übertragung
In den in Kapitel 2.1.3.2 beschriebenen Multi-Hop-Netzwerken muß auf Grund der Mobilität mobiler Endsysteme, die mittels ihrer Forwarding-Funktionalität die Weiterleitung von Paketen übernehmen, das Routing häufig angepaßt werden. Im Kontext vieler, sich schnell bewegender mobiler Systeme sind kurzzeitige Unterbrechungen und somit deutlich höhere Paketverlustraten als in drahtgebundenen Netzen die Folge [DPR00], [BMJ+98]. Darüber hinaus

sind unter Umständen auch länger andauernde Unterbrechungen der Netzwerkkonnektivität für mobile Endsysteme unvermeidbar. Dies ist für ein Endsystem A der Fall, falls ein Endsystem B, das ursprünglich das Forwarding zu Endsystem A übernommen hat, auf Grund eines Ortswechsels Pakete nicht mehr zu Endsystem A weiterleiten kann und auch kein anderes mobiles Endsystem des Multi-Hop-Netzwerkes das Weiterleiten zu Endsystem A übernehmen kann. Ein zwischenzeitlicher Verlust der Netzwerkkonnektivität stellt in Multi-Hop-Netzwerken keine Ausnahmesituation dar. Bei Infrastrukturnetzwerken können Basisstationswechsel einen – allerdings kurzzeitigen – Verlust der Netzwerkkonnektivität zur Folge haben. Sowohl bei Multi-Hop-Netzwerken als auch bei Infrastrukturnetzwerken ist das temporäre Verlassen des Bereiches der Netzabdeckung seitens eines mobilen Systems unter Umständen nicht zu vermeiden. Auch in diesem Fall ist ein temporärer Verlust der Netzwerkkonnektivität die Folge.

Funkkanäle sind hinsichtlich Übertragungsfehlern wesentlich anfälliger als drahtgebundene Übertragungskanäle. Vorwärtsfehlerkorrektur und eine geeignete Wahl des auf dem Funkkanal verwendeten Kodierungsverfahrens werden eingesetzt, um die für höhere Schichten des Protokollstacks sichtbare Bitfehlerrate zu reduzieren. Vorwärtsfehlerkorrekturverfahren fügen dem Datenstrom Redundanz hinzu, die beim Empfänger zur Korrektur von Bitfehlern genutzt werden kann. Intelligente Verfahren adaptieren die Menge hinzugefügter Redundanz unter Berücksichtigung der aktuellen Übertragungseigenschaften des Funkkanals. Somit kann vermieden werden, daß zu Zeiten guter Übertragungseigenschaften unnötigerweise Redundanz hinzugefügt und somit Übertragungsbandbreite verschwendet wird.

Im Rahmen der vorliegenden Arbeit wird davon ausgegangen, daß der Funkkanal trotz Vorwärtsfehlerkorrektur nicht jederzeit die Übertragung mit Bitfehlerraten ermöglicht, wie sie bei der drahtgebundenen Übertragung anzutreffen sind. Um diese Annahme zu untermauern, wird im folgenden auf Vermessungen installierter drahtloser Kommunikationssysteme [DR92], [ES96], [RSW98], [CG97], in der Spezifikation der Systeme aufgeführte Angaben [Wav96] und auf für die Modellierung derartiger Systeme verwendete Modelle [ES98a] eingegangen.

Bitfehlerraten bzw. Paketverlustraten, die sich mittels geeigneter Kanalkodierungsverfahren und Vorwärtsfehlerkorrekturverfahren – aber ohne vom System ggf. unterstützte Schicht 2 Übertragungswiederholungen – erzielen lassen, sind für einige Systeme im folgenden aufgeführt. Bei Systemen mit Schicht 2 Wiederholungen kann lediglich die verbleibende Fehlerrate bestimmt werden, die sich ergibt, nachdem bereits Fehler mittels Schicht 2 Wiederholungen korrigiert wurden, aber nicht die alleine durch Kanalkodierungsverfahren und Vorwärtsfehlerkorrekturverfahren erzielbaren Bitfehlerraten. Da bei den folgenden Ausführungen die typischerweise auf dem Funkkanal auftretenden Fehlerraten Gegenstand der Betrachtungen sind, wird auf Systeme mit Schicht 2 Wiederholungen in diesem Unterkapitel nicht weiter eingegangen. Übertragungswiederholungen in der Schicht 2 werden in Kapitel 3.3.1 als eine von mehreren Möglichkeiten zur Kompensation fehleranfälliger drahtloser Links diskutiert. Dort wird auch beschrieben, welche negativen Auswirkungen sie unter Umständen haben.

Das drahtlose lokale Netz WaveLAN [Wav96] ist in mehreren verschiedenen Untersuchungen hinsichtlich Übertragungsfehlern betrachtet worden. [DR92] beschreibt die Paketfehlerwahrscheinlichkeit des im Frequenzbereich um 900 MHz betriebenen WaveLANs in Abhängigkeit von der Distanz zwischen Sender und Empfänger. Zwischen Sender und Empfänger, die innerhalb eines Gebäudes auf einem Gang angeordnet sind, besteht eine Sichtverbindung. Bis zu einer Entfernung von 40 Metern liegt die Paketfehlerwahrscheinlichkeit unter 1 Prozent und zwischen 40 und 50 Metern unter 2 Prozent. Im Bereich zwischen 50 und 55 Metern steigt

sie auf bis zu 60 Prozent an. Darüber hinaus schwankt die Fehlerrate in diesem Bereich stark. Bereits kleine Positionsänderungen haben unter Umständen eine starke Veränderung der Paketfehlerwahrscheinlichkeit zur Folge. Eine geringere Distanz bedeutet hierbei allerdings nicht auch zugleich eine geringere Paketfehlerwahrscheinlichkeit.

[ES96] beschreibt ebenfalls die Messungen an einem installierten WaveLAN. Es werden in einer Büroumgebung verschiedene typische Szenarien betrachtet und für diese die Paketfehlerwahrscheinlichkeiten bestimmt. Reichweitenbetrachtungen sind nicht im Fokus dieser Untersuchungen, stattdessen werden die Auswirkungen von Hindernissen im Ausbreitungspfad der Funkwellen und die Interferenz mit Signalen anderer den gleichen Frequenzbereich nutzenden Sendern betrachtet. Für einen ca. 3 Meter entfernten und durch eine Wand vom Sender getrennten Empfänger ermitteln die Autoren eine Paketfehlerwahrscheinlichkeit nahe Null. In weiteren Szenarien, bei denen die Distanz zwischen 10 und 15 Metern variiert und bis zu 3 Wände zwischen Sender und Empfänger angeordnet sind, ergeben sich Paketverlustraten von bis zu 3 Prozent. Darüber hinaus beschreiben die Autoren ein Szenario, in dem Sender und Empfänger ohne Paketverluste miteinander kommunizieren können, und sich alleine dadurch, daß sich ein Mensch über die Antenne des Empfängers beugt, eine Paketfehlerwahrscheinlichkeit von 15 Prozent ergibt. Das Einschalten eines drahtlosen Inhouse-Telefons, das im gleichen Frequenzbereich betrieben wird, verursacht ein Ansteigen der Paketfehlerwahrscheinlichkeit auf über 50 Prozent. Diese Messungen fließen in ein Fehlermodell ein, das Bitfehlerraten zwischen 0 und 10^{-3} annimmt und in [ES98a] beschrieben ist. Auch die in [RSW98] beschriebenen Messungen zeigen eine große Schwankungsbreite der Paketfehlerraten. An Orten mit optimalem Funkempfang liegt sie bei 0 Prozent, an weniger günstigen Orten bei 5 Prozent und an Orten mit schlechtem Funkempfang bei bis zu 40 Prozent. Vor dem Hintergrund all dieser Messungen muß die vom Hersteller für WaveLAN angegebene Bitfehlerrate von 10^{-8} [Wav96] als zu optimistisch und nur unter optimalen Bedingungen erreichbar angesehen werden.

Mittels Übertragungswiederholungen lassen sich auch an Orten schlechten Funkempfangs niedrige Paketfehlerraten erzielen. In [RSW98] werden für das drahtlose lokale Netz ARLAN [ARL97] Paketfehlerraten von 10^{-6} angegeben. In [Wav99] wird für WaveLAN IEEE 802.11 bzw. IEEE 802.11b eine Bitfehlerrate von kleiner als 10^{-5} genannt. Auf die Übertragungsfehlerwahrscheinlichkeit dieser Systeme wird hier nicht weiter eingegangen, da sie bereits spezielle Mechanismen zur Kompensation der höheren Fehlerraten auf dem Funkkanal beinhalten. Zusammen mit anderen Mechanismen, die die höhere Fehleranfälligkeit des drahtlosen Links adressieren, werden sie in Kapitel 3 beschrieben.

Hinsichtlich der Bitfehlerraten stellt sich die Situation in drahtlosen Netzen, die eine überregionale Funkabdeckung bieten, ähnlich dar. Im sogenannten transparenten Übertragungsmodus von GSM, der auf lokale Übertragungswiederholungen in der Schicht 2 verzichtet, ergeben sich Bitfehlerraten im Bereich von 10^{-2} bis 10^{-5} [EV97]. Für den in der GSM Phase 2+ neu eingeführten General Packet Radio Service (GPRS) [BW97], [CG97] wird von Bitfehlerraten im Bereich von 10^{-3} bis 10^{-6} ausgegangen.

In Tabelle 2.2 sind nochmals die Ursachen für temporäre Unterbrechungen und temporär höhere Bitfehlerraten zusammengefaßt. Unterbrechungen und höhere Bitfehlerraten sind nicht als anormal anzusehen, sondern können sich im Falle der funkbasierten Übertragung auch unter normalen Umständen ergeben. Diese *Schwankungen der Übertragungseigenschaften* sind typisch für die drahtlose Kommunikation. Um trotz dieser Schwankungen der Übertragungseigenschaften eine zuverlässige Kommunikation zu ermöglichen, muß sich ein System an die aktuellen Übertragungseigenschaften adaptieren können.

temporäre Unterbrechungen (Verlust der Netzwerkkonnektivität)	temporär höhere Bitfehlerraten
unvollständige Netzabdeckung	Erreichen der Reichweitengrenze
Fehlende Weiterleitung in Multi-Hop-Netzwerken	Funksender im gleichen Frequenzband (z.B. ISM-Band)
Basisstationswechsel	Abschattungseffekte

Tabelle 2.2: Ursachen für Unterbrechungen bzw. höhere Bitfehlerraten

2.1.5 Kopplung verschiedener Infrastrukturnetzwerke

Abb. 2.5 zeigt ein Szenario, in dem mehrere verschiedene Infrastrukturnetzwerke über das Internet gekoppelt sind. Der lokale Bereich wird im dargestellten Szenario durch zwei drahtlose lokale Netze (IEEE 802.11) mit hohen zur Verfügung gestellten Übertragungsraten abgedeckt. Eine flächendeckende Netzabdeckung und geringere Übertragungsraten bietet das terrestrische Mobilkommunikationssystem GSM. Die beiden drahtlosen lokalen Netze verwenden im dargestellten Szenario identische Netzwerktechnologien, sind aber verschiedenen administrativen Domänen zugeordnet. Der Laptop ist mit 2 Netzwerkkarten ausgerüstet: Einer IEEE 802.11 Karte und einer Karte für den Zugang zu dem GSM-Netz.

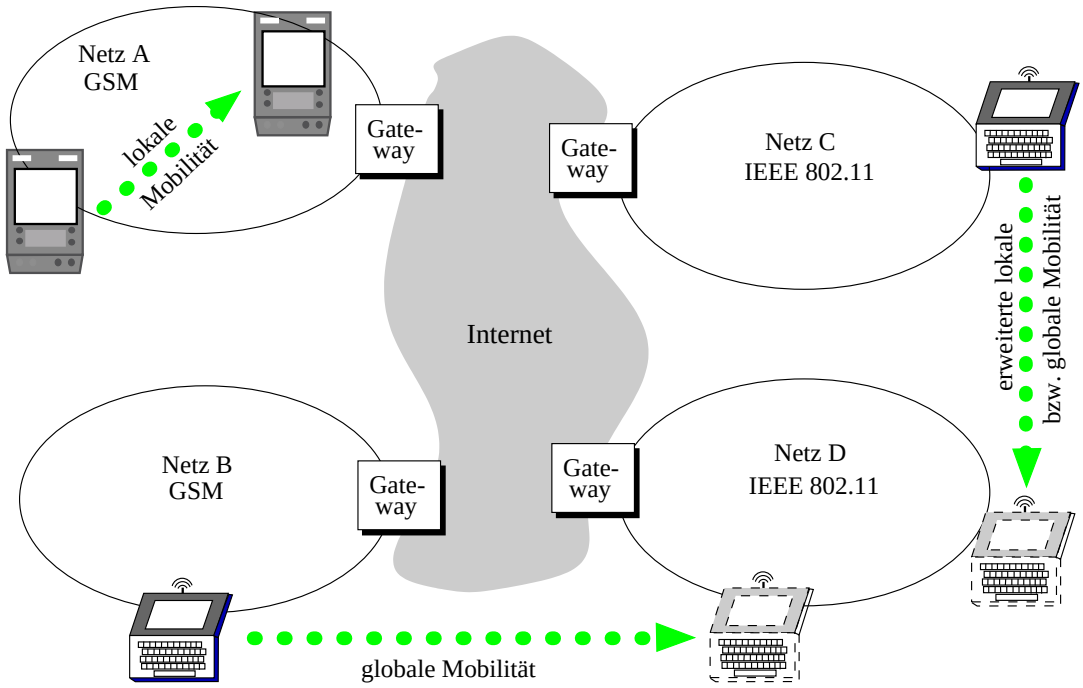


Abbildung 2.5: Kopplung verschiedener Infrastrukturnetzwerke

In Abb. 2.5 sind drei Arten der Mobilität dargestellt, die im folgenden erläutert werden:

- Lokale Mobilität
  Die Mobilität des mobilen Systems ist auf den Abdeckungsbereich eines Infrastrukturnetzwerkes limitiert. Ist die Mobilität des Palmtop wie in Abb. 2.5 dargestellt auf das Netz A beschränkt, ist hierfür lediglich eine *lokale Mobilitätsunterstützung* erforderlich. In Netz B, Netz C und Netz D hat der Palmtop keine Netzwerkkonnektivität. Die lokale

Mobilität kann alleine durch die Mobilitätsunterstützung innerhalb des jeweiligen Netzes realisiert werden. Eine Abstimmung bzw. Standardisierung zwischen verschiedenen Netzen ist nicht erforderlich, d.h. proprietäre Einzellösungen sind möglich.

- Erweiterte lokale Mobilitätsunterstützung
  Im Gegensatz zur lokalen Mobilität ist die Mobilität des Endsystems nicht auf genau ein Infrastrukturnetzwerk beschränkt. Verwenden mehrere Infrastrukturnetzwerke die gleiche Funktechnologie und gibt es Übereinkünfte zwischen den Betreibern hinsichtlich einer Mobilitätsunterstützung zwischen diesen Netzwerken, so spricht man von einer *erweiterten lokalen Mobilitätsunterstützung*. Im in Abb. 2.5 skizzierten Szenario existiert ein derartiges Abkommen zwischen den Betreibern des Netzes C und des Netzes D, so daß trotz des Wechsels des Laptops von Netz C in Netz D die Netzwerkkonnektivität bestehen bleibt. Im Bereich der mobilen Telefonie gibt es Abkommen zwischen Providern, die das sogenannte *Roaming*, d.h. den Wechsel eines Mobiltelefons vom Netz eines Providers in das Netz eines anderen Providers, regeln.

- Globale Mobilitätsunterstützung
  Globale Mobilität liegt vor, falls ein Endsystem in den Bereich eines anderen Infrastrukturnetzwerkes wechselt, welches eine andere Funktechnologie nutzt. Für den Laptop, der in Abb. 2.5 Netz B verläßt und sich in Netz D anmeldet, ist eine *globale Mobilitätsunterstützung* notwendig, um die Netzwerkkonnektivität aufrechtzuerhalten.

  Globale Mobilität liegt allerdings nicht nur dann vor, wenn mit dem Netzwerkwechsel auch ein Wechsel der Funktechnologie einhergeht. Unter der Annahme, daß im in Abb. 2.5 skizzierten Szenario keine Übereinkünfte hinsichtlich der Mobilitätsunterstützung zwischen den Betreibern von Netz C und Netz D existieren, kann der Laptop nicht von einer erweiterten lokalen Mobilitätsunterstützung profitieren. Stattdessen ist der Laptop auf eine globale Mobilitätsunterstützung angewiesen, um auch nach einem Wechsel in Netz D die Netzwerkkonnektivität aufrechterhalten zu können.

Auch in Zukunft ist nicht davon auszugehen, daß die drahtlose Anbindung mobiler Systeme durch ein einziges Infrastrukturnetzwerk realisiert werden wird. Somit ist eine lokale bzw. erweiterte lokale Mobilitätsunterstützung für die Internetanbindung mobiler Systeme nicht ausreichend, sondern eine globale Mobilitätsunterstützung erforderlich. Aufgabe der globalen Unterstützung ist es, für mobile Systeme bestimmte IP-Pakete über die IP-Router des Internets zum Gateway des Infrastrukturnetzwerkes zu routen, über das die drahtlose Anbindung der mobilen Systeme erfolgt. Innerhalb des jeweiligen Infrastrukturnetzwerkes obliegt es der lokalen bzw. erweiterten lokalen Mobilitätsunterstützung des jeweiligen Infrastrukturnetzwerkes, die IP-Pakete weiter zum jeweiligen mobilen System zu transportieren.

Die Konzepte der lokalen Mobilitätsunterstützung sind spezifisch für das jeweils verwendete Infrastrukturnetzwerk. Die globale Mobilitätsunterstützung hingegen ist zugeschnitten auf die die verschiedenen Infrastrukturnetzwerke verbindende Netzwerktechnologie, d.h. das Internet. Für eine globale Mobilitätsunterstützung sind somit Mechanismen notwendig, die die Adressierung mobiler IP-basierter Endsysteme im Internet erlauben und die IP-Pakete zu dem Gateway des Infrastrukturnetzwerkes routen, über das das mobile System aktuell angebunden ist. Das von der IETF entwickelte und in [Per96b] spezifizierte Mobile IP Protokoll bietet diese Funktionalität und wird im folgenden Unterkapitel in seinen Grundzügen beschrieben.

2.2 Globale Mobilitätsunterstützung: Mobile IP

Erste Ideen für eine globale Mobilitätsunterstützung im Internet sind in [IDJ92] beschrieben. Von verschiedenen Forschungseinrichtungen wurden mehrere Konzepte entwickelt. Ein Überblick über diese Ansätze ist in [SZD96], eine vergleichende Gegenüberstellung in [FZ96] zu finden. Als das Protokoll der Wahl hat sich das Mobile IP Protokoll herauskristallisiert. Es ist in RFC 2002 [Per96b] und in [Per98a] im Detail beschrieben. Um einen Überblick über Mobile IP, d.h. die verwendete Architektur und die wesentlichen Protokollfunktionen, zu gewinnen, eignet sich [Per98b]. Die Grundzüge des IP-Routings [Hui00], die Architektur von Mobile IP und die wesentlichen Protokollmechanismen von Mobile IP werden in diesem Unterkapitel insoweit beschrieben, wie es für das Verständnis der vorliegenden Arbeit erforderlich ist.

2.2.1 Grundproblem

Hauptproblem bei der Internetanbindung mobiler Systeme ist die Tatsache, daß ohne Mobilitätsunterstützung IP-Pakete, die an ein mobiles System adressiert sind, unter Umständen nicht an den aktuellen Aufenthaltsort des mobilen Systems geroutet werden. Router im Internet bestimmen anhand der in der Routingtabelle gespeicherten Information aus der im IP-Paket kodierten *Zieladresse* eines Pakets den nächsten Router, an den das Paket weitergeleitet wird. Falls weder die IP-Adresse eines mobilen Systems noch Routingtabelleneinträge modifiziert werden, ändert sich auch das Routing der an das mobile System adressierten Pakete nicht. Somit werden nach einem Ortswechsel Pakete nicht an den neuen Aufenthaltsort eines mobilen Systems transportiert.

Adressierung in IP-Netzwerken
Die Adressierung im Internet erfolgt anhand einer 32 Bits umfassenden IP-Adresse. Anstatt IP-Adressen binär darzustellen, werden zur besseren Lesbarkeit in der Regel jeweils 8 Bits zusammengefaßt, als Dezimalwert dargestellt und die sich ergebenden 4 Dezimalwerte durch Punkte voneinander getrennt. Diese Notation wird als Punktnotation bezeichnet. 134.169.34.1 ist beispielsweise die Darstellung einer IP-Adresse in der Punktnotation.

Hinsichtlich der Routingstrategien wird zwischen dem *flachen Routing* und dem *Präfix-Routing* unterschieden. Beim flachen Routing ist die vollständige IP-Adresse Grundlage für die Routingentscheidung innerhalb eines Routers. In jedem Router muß für jedes adressierbare System ein Routingtabelleneintrag vorhanden sein. Aufgrund der linear mit der Anzahl der adressierbaren Endsysteme steigenden Größe der Routingtabellen skaliert dieser Ansatz nicht.

Die Idee des Präfix-Routings ist es, in den IP-Routern Routinginformationen zu aggregieren. Grundkonzept hierbei ist, für Systeme, deren Pakete über den gleichen nächsten Router weitergeleitet werden, nicht jeweils einen individuellen Eintrag in der Routingtabelle zu verwenden, sondern einen Eintrag für mehrere Endsysteme zu nutzen. Die Routingentscheidung erfolgt dann allerdings nicht auf Grundlage der kompletten IP-Adresse, sondern auf Basis des sogenannten *Routing-Präfixes*. Der Routing-Präfix setzt sich aus einer IP-Adresse und der Angabe der Anzahl der relevanten höherwertigen Bits zusammen. Der Präfix 134.169.34/24 umfaßt beispielsweise die 24 höherwertigen Bits der angeführten Adresse. Für Endsysteme mit verschiedenen IP-Adressen, aber identischem Routing-Präfix ist in der Routingtabelle

nur ein Eintrag erforderlich. Diese Systeme müssen geographisch so ans Internet angebunden sein, daß sie auch tatsächlich über denselben nächsten Router erreicht werden können. Beim Präfix-Routing reflektiert der Routing-Präfix einer IP-Adresse zugleich auch, wo in der Netzwerktopologie das jeweilige Endsystem an das Internet angebunden ist. Ohne Änderung der IP-Adresse – und somit auch des Routing-Präfixes – kann ein Endsystem nicht an einer anderen Stelle in der Netzwerktopologie an das Internet angebunden werden, da andernfalls für dieses Endsystem bestimmte Pakete nicht an diesen Ort geroutet werden würden. Eine Beschreibung der derzeit im Internet für das Routing verwendeten Konzepte ist in [Hui00] zu finden. Details bezüglich des verwendeten Routings auf Basis des *Classless Inter-Domain Routings* (CIDR) können RFC 1518 [RL93] entnommen werden. Für den Austausch der für das Routing erforderlichen Informationen kann das *Border Gateway Protocol* (BGP) [RL94] eingesetzt werden.

Empfängt ein Router ein Paket, das nicht an ihn selbst adressiert ist, ist er für das Routing dieses Pakets zuständig. Zur Bestimmung, an welches System das Paket weiterzuleiten ist, wird die Routingtabelle herangezogen. Unter anderem enthält eine Zeile dieser Tabelle einen Routing-Präfix und die IP-Adresse des Routers, an den das jeweilige Paket weiterzuleiten ist. Für jedes weiterzuleitende Paket wird die IP-Adresse des Pakets mit den in der Tabelle gespeicherten Präfixes verglichen und der längste übereinstimmende Routing-Präfix ermittelt. An den in der zugehörigen Zeile der Routingtabelle aufgeführten Router wird das Paket gesendet.

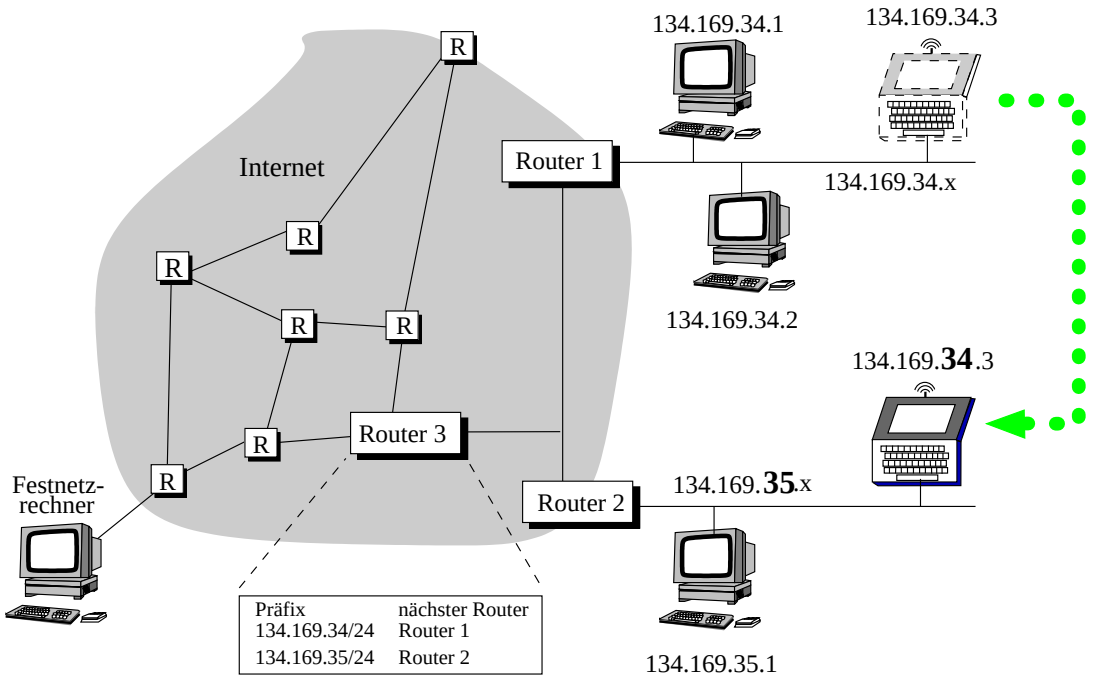


Abbildung 2.6: Routing in IP-Netzwerken

Abb. 2.6 zeigt ein Szenario mit einem Festnetzrechner, mehreren Routern, zwei Subnetzen und einem mobilen Laptop, der mit dem Festnetzrechner kommuniziert. Die zwei dargestellten Subnetze sind über Router 1 bzw. Router 2 und diese über Router 3 an das Internet angebunden. In Router 3 wird entschieden, in welches der beiden dargestellten Subnetze ein Paket weitergeleitet wird. Grundlage hierfür sind die in der Abbildung dargestellten Zeilen der Routingtabelle. Pakete mit der Zieladresse 134.169.34.x werden an Router 1 gesendet,

Pakete mit der Zieladresse 134.169.35.x an Router 2. Die bereits angesprochene Aggregation von Routinginformation äußert sich darin, daß unabhängig von der Anzahl der in den dargestellten Subnetzen angeschlossenen Endsysteme jeweils nur ein Eintrag in der Routingtabelle von Router 3 erforderlich ist.

IP-Routing zu mobilen Systemen

Ist der Laptop mit der IP-Adresse 134.169.34.3 über das Subnetz 134.169.34.x an das Internet angebunden, so werden an ihn adressierte Pakete korrekt bei ihm ausgeliefert. Ist der Laptop hingegen nach einem Ortswechsel, wie in Abb. 2.6 schematisch dargestellt, über das Subnetz 134.169.35.x an das Internet angebunden, ist er aus dem Internet nicht mehr erreichbar. Ursache hierfür ist der Routing-Präfix der IP-Adresse des Laptops, der nicht zum Präfix des Subnetzes, in das er gewechselt ist, paßt. An den Laptop gesendete IP-Pakete werden weiterhin über den Router 1 in das Subnetz 134.169.34.x ausgeliefert.

Ein erster Ansatz, um die Erreichbarkeit eines mobilen Systems auch nach einem Subnetzwechsel sicherzustellen, ist es, dem mobilen System eine neue IP-Adresse zuzuweisen, deren Routing-Präfix zu dem Präfix des neuen Subnetzes paßt. Somit hat ein Subnetzwechsel auch einen Wechsel der IP-Adresse des mobilen Systems zur Folge. Eine Änderung der IP-Adresse ist allerdings für bereits laufende Anwendungen problematisch. Beim Start einer Kommunikationsbeziehung werden im mobilen System im sogenannten Protokollkontrollblock, in dem Statusinformation des verwendeten Transportprotokolls verwaltet wird, unter anderem die IP-Adressen der miteinander kommunizierenden Endsysteme abgelegt. Zusammen mit einem weiteren Identifer, der sogenannten Portnummer, kann ein einzelner Verbindungsendpunkt identifiziert werden. Ändert sich die IP-Adresse, so kann das empfangende Endsystem auf Grund der geänderten IP-Adresse das IP-Paket nicht mehr der jeweiligen Kommunikationsbeziehung zuordnen. Als Konsequenz ergibt sich hieraus die Notwendigkeit eines Neustartes der Kommunikationsbeziehung und ggf. der jeweiligen Anwendung. Wegen dieses Neustartes kann durch den beschriebenen Ansatz lediglich Portabilität, aber nicht Mobilität von Endsystemen unterstützt werden.

Wie beschrieben, ist die IP-Adresse für das Routing im Internet von Bedeutung, darüber hinaus ist sie auch für die Identifikation von Verbindungsendpunkten relevant. Für die Unterstützung mobiler Endsysteme ergeben sich zwei nicht miteinander vereinbare Randbedingungen: Während der Verbindungsendpunkt (und damit auch die IP-Adresse), den die Anwendungen für ihre Kommunikation nutzen, auch im Fall von Subnetzwechseln eines mobilen Systems unverändert bleiben muß, ist für das korrekte Routing der Pakete in das neue Subnetz eine Änderung der IP-Adresse erforderlich.

Die Grundidee für die Lösung dieses Problems besteht darin, dem mobilen System zwei Adressen zuzuordnen. Eine *permanente IP-Adresse*, die auch im Falle von Subnetzwechseln nicht geändert wird, dient der Identifikation des Verbindungsendpunktes. Die zweite Adresse wird als *temporäre IP-Adresse* bezeichnet und ist für das Routing der Pakete zum aktuellen Aufenthaltsort des mobilen Endsystems relevant. Für das Mapping zwischen der permanenten und der temporären Adresse ist im Netzwerk eine Instanz erforderlich, die beide Adressen kennt und insbesondere auch über die Änderung der temporären IP-Adresse nach einem Subnetzwechsel informiert wird.

2.2.2 Architektur und grundlegender Protokollablauf

Für die Mobilitätsunterstützung sind in Mobile IP zwei ausgewiesene Systeme vorgesehen, die sogenannten *Mobility Agents*. Das Mobile IP Protokoll operiert zwischen diesen Systemen und dem mobilen Endsystem. Auf den Festnetzrechnern, zu denen das mobile System Transportverbindungen unterhält, ist keine Mobile IP Implementierung erforderlich. Die für die Mobilitätsunterstützung notwendigen Änderungen beschränken sich somit auf das mobile System und die im folgenden beschriebenen Mobility Agents von Mobile IP:

- Home Agent
  Mobilen Systemen wird eine *permanente IP-Adresse* zugewiesen. Das Subnetz, zu dem diese IP-Adresse gehört, wird als das *Heimatsubnetz* eines mobilen Systems bezeichnet. Um für ein mobiles System eine Mobilitätsunterstützung zu realisieren, ist in dem zugehörigen Heimatsubnetz ein *Home Agent* notwendig. Es ist Aufgabe des Home Agents, die für ein mobiles System bestimmten IP-Pakete in das Subnetz weiterzuleiten, in dem das mobile System aktuell an das Internet angebunden ist. In diesem Subnetz übernimmt der Foreign Agent den Weitertransport der IP-Pakete.

- Foreign Agent
  Ist ein mobiles System entfernt von seinem Heimatsubnetz an das Internet angebunden, so übernimmt ein im sogenannten *fremden Subnetz* angesiedelter *Foreign Agent* die Mobilitätsunterstützung. Er empfängt die für das mobile System vom Home Agent weitergeleiteten IP-Pakete und liefert sie an das mobile System aus. Darüber hinaus sind Foreign Agents in den Prozeß der Anmeldung eines mobilen Endsystems nach einem Subnetzwechsel involviert.

Abb. 2.7 zeigt ein Szenario mit einem Heimatsubnetz, zwei fremden Subnetzen und den zugehörigen Mobility Agents. Im Heimatsubnetz ist ein Home Agent realisiert. Im fremden Subnetz B ist für die Mobilitätsunterstützung ein Foreign Agent verfügbar, im fremden Subnetz C hingegen nicht. Der Home Agent bzw. der Foreign Agent müssen nicht unbedingt wie im Szenario dargestellt auf einem System innerhalb des Subnetzes realisiert sein, sondern können auch direkt auf einem das Subnetz an das Internet anbindenden Router plaziert werden.

Für die Realisierung der Mobilitätsunterstützung stellt Mobile IP Mechanismen für das *Agent Discovery*, die *Registrierung* und das *Mobile IP Routing* bereit. Der grundlegende Ablauf, wie mit diesen Mechanismen eine globale Mobilitätsunterstützung realisiert werden kann, wird im nächsten Unterkapitel skizziert. Eine detaillierte Beschreibung der einzelnen Funktionen und ihre protokolltechnischen Umsetzung erfolgt in Kapitel 2.2.3.

2.2.2.1 Grundlegender Protokollablauf

Das mobile System ist in Abb. 2.7 zunächst in seinem Heimatsubnetz an das Internet angebunden. Eine spezielle Mobilitätsunterstützung ist in diesem Fall nicht notwendig, da an die permanente IP-Adresse des mobilen Systems adressierte Pakete in das Heimatsubnetz geroutet werden. Der im Heimatsubnetz angesiedelte Home Agent ist nur in die Mobilitätsunterstützung involviert, falls sich das unterstützte mobile System in einem fremden Subnetz aufhält. Kehrt das mobile System aus einem fremden Subnetz in sein Heimatsubnetz zurück, beendet

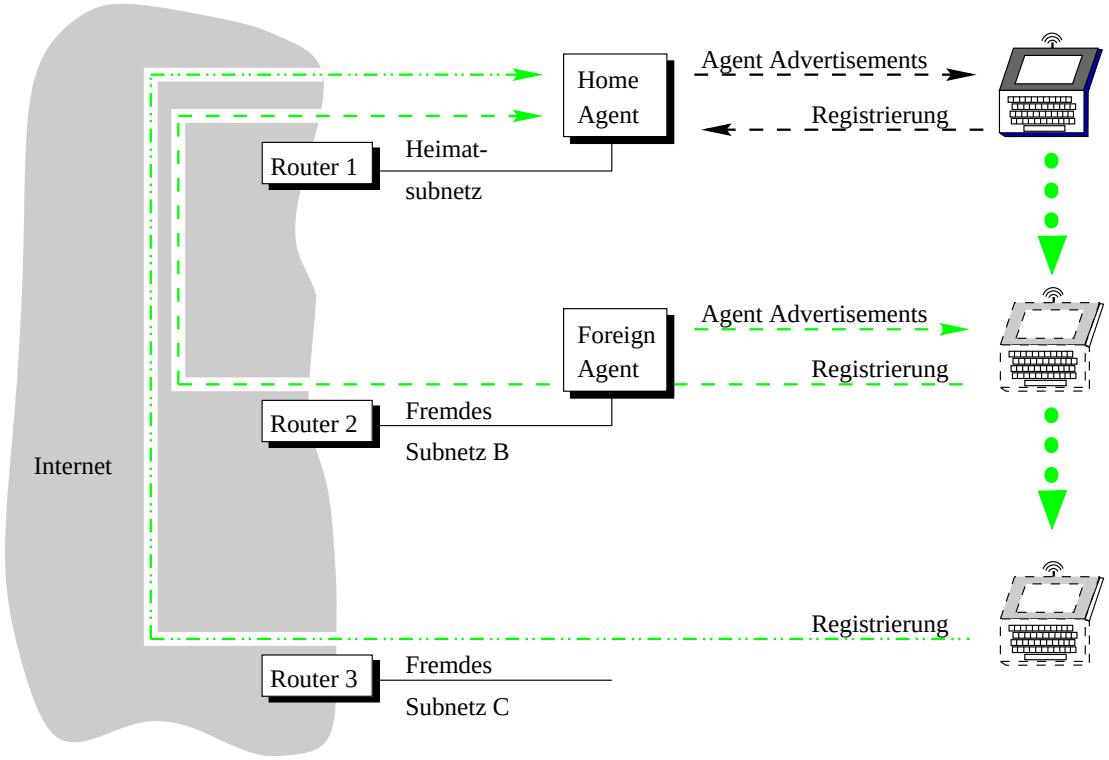


Abbildung 2.7: Mobile IP

der Home Agent seine Unterstützung, d.h. das mobile System ist auch ohne Beteiligung des Home Agents aus dem Internet erreichbar. Nach einem Subnetzwechsel ermittelt ein mobiles System zunächst mittels des *Agent Discoverys*, ob ein Foreign Agent im neuen Subnetz verfügbar ist. Mittels der *Registrierung* beim Home Agent wird dieser darüber informiert, zu welchem System er an das mobile Endsystem adressierte IP-Pakete weiterleiten soll. Aufgabe des *Mobile IP Routings* ist es, diese IP-Pakete in das Subnetz zu routen, in dem das mobile System aktuell an das Internet angebunden ist. Da der Routing-Präfix der permanenten IP-Adresse nicht zum Subnetz paßt, sind hierfür spezielle Mechanismen notwendig.

Agent Discovery
Foreign Agents und Home Agents senden periodisch sogenannte *Agent Advertisements* per Multicast aus. Diese Agent Advertisements werden in das Subnetz gesendet, für das das jeweilige System als Agent fungiert. Eine Weiterleitung der Advertisements in andere Subnetze erfolgt nicht. In den Advertisements ist unter anderem das Subnetz, in dem der Agent positioniert ist, kodiert, so daß das mobile System durch Auswertung dieser Advertisements erkennen kann, ob ein Subnetzwechsel stattgefunden hat. Darüber hinaus kann es ermitteln, ob es in ein fremdes Subnetz oder in sein Heimatsubnetz gewechselt ist. Ist ein Subnetzwechsel erfolgt, veranlaßt das mobile System eine Registrierung beim Home Agent. Neben der Möglichkeit der periodischen Übertragung der Advertisements kann ein mobiles System auch die Übertragung eines Advertisements explizit anfordern. Ein detaillierte Beschreibung der Agent-Discovery-Mechanismen erfolgt in Kapitel 2.2.3.1.

Registrierung
Hinsichtlich der Registrierung muß unterschieden werden, ob ein mobiles System in sein Heimatsubnetz zurückgekehrt oder in ein fremdes Subnetz gewechselt ist. Ist ein mobiles Endsystem in ein fremdes Subnetz gewechselt, so wird dort ein System für die Mobilitätsunterstützung bestimmt. Die IP-Adresse dieses Systems wird als *Care-of-Adresse* bezeichnet. Sie wird als *temporäre IP-Adresse* des mobilen Systems verwendet. Mittels einer Registrierung beim Home Agent wird dieser über die Care-of-Adresse informiert. Der Home Agent richtet daraufhin die Mobilitätsunterstützung für das mobile System ein und sendet die an das mobile System adressierten IP-Pakete mittels des im nächsten Abschnitt beschriebenen Mobile IP Routings an die Care-of-Adresse. Wechselt das mobile System von einem fremden Subnetz zurück in sein Heimatsubnetz, so wird die Weiterleitung in das fremde Subnetz, in dem das mobile System vorher registriert war, deaktiviert. Die IP-Pakete werden im Heimatsubnetz ausgeliefert. Registrierungen werden über UDP zwischen dem mobilen System und dem Home Agent ausgetauscht; sie sind im Detail in Kapitel 2.2.3.2 beschrieben.

Mobile IP Routing
An die *permanente IP-Adresse* eines mobilen Systems adressierte IP-Pakete werden in das Heimatsubnetz des mobilen Systems geroutet. Ist das mobile Endsystem nicht in seinem Heimatsubnetz registriert, so kann es die IP-Pakete nicht empfangen. In Mobile IP ist es die Aufgabe des Home Agents, diese IP-Pakete in Empfang zu nehmen. Hierzu bedient sich der Home Agent der Mechanismen proxy ARP [Pos84] und gratuitous ARP [Ste94], um die eigentlich an das mobile System adressierten IP-Pakete zu empfangen. Mit dem Wissen, in welchem Subnetz das mobile System zur Zeit registriert ist, kann der Home Agent diese Pakete in dieses Subnetz weiterleiten. Ein sogenannter *Tunnel* wird dazu eingesetzt, um IP-Pakete, die eigentlich an die permanente IP-Adresse des mobilen Endsystems adressiert sind, an die Care-of-Adresse zu senden. Hierbei werden die für das mobile Endsystem bestimmten IP-Pakete in ein neues Paket eingekapselt. Als Absenderadresse des neuen Pakets wird die IP-Adresse des Home Agents, als Zieladresse die Care-of-Adresse verwendet. Der *Tunnelanfangspunkt* ist somit bei dem Home Agent, der *Tunnelendpunkt* ist bei dem System, dessen IP-Adresse als Care-of-Adresse dient.

Bei der Übertragung von IP-Paketen, die vom mobilen System gesendet werden, greift Mobile IP nicht in das Routing ein. IP-Pakete werden genauso behandelt, als ob sie von einem nicht mobilen System gesendet worden wären. Insbesondere werden sie nicht erst über den Home Agent geroutet. Dieses asymmetrische Routing wird im Kontext von Mobile IP auch als *Dreiecksrouting* bezeichnet.

2.2.2.2 Operationsmodi von Mobile IP

Mobile IP bietet zwei verschiedene Operationsmodi: Den *Foreign-Agent-Modus* und den *Colocated-Modus*. In beiden Modi ist die Existenz eines Home Agents für die Mobilitätsunterstützung notwendig. Die Modi unterscheiden sich dahingehend, zu welchem im fremden Subnetz angesiedelten System die für das mobile System bestimmten IP-Pakete vom Home Agent weitergeleitet werden. Dieses System fungiert dann als Tunnelendpunkt für Mobile IP. Die Existenz eines Foreign Agents im fremden Subnetz ist nicht zwingend für den Einsatz von Mobile IP notwendig. Ist ein Foreign Agent in dem Subnetz, in das ein mobiles System gewech-

selt ist, vorhanden, so kann der Foreign-Agent-Modus oder der Colocated-Modus eingesetzt werden.

- Colocated-Modus
  Dieser Modus erlaubt es, auch dann eine Mobilitätsunterstützung zu bieten, falls in einem fremden Subnetz kein Foreign Agent verfügbar ist. Hierzu wird dem mobilen System zusätzlich zur permanenten IP-Adresse eine zu dem fremden Subnetz passende temporäre IP-Adresse – beispielsweise mittels DHCP [PJ95] – zugewiesen. Diese neu zugewiesene IP-Adresse wird als Care-of-Adresse verwendet. An das mobile System adressierte IP-Pakete werden somit von dem Home Agent direkt bis zum mobilen System getunnelt, d.h. das mobile System dient als Tunnelendpunkt. In Abb. 2.7 nutzt der Laptop in Subnetz C den Colocated-Modus. Wesentlicher Nachteil dieses Modus ist die Tatsache, daß für jedes mobile System zusätzlich eine zum fremden Subnetz passende IP-Adresse vergeben werden muß. Insbesondere vor dem Hintergrund der Verknappung der im IPv4-Adreßraum verfügbaren Adressen, sollte dieser Modus nur dann Anwendung finden, falls kein Foreign Agent im fremden Subnetz verfügbar ist. Darüber hinaus beansprucht die Übertragung des für das Tunneln zusätzlich erforderlichen IP-Paketkopfes Übertragungsbandbreite auf dem drahtlosen Link. Insbesondere im Falle geringer zur Verfügung stehender Bandbreiten ist dies problematisch.

- Foreign-Agent-Modus
  Der Foreign-Agent-Modus setzt die Existenz eines Foreign Agents im fremden Subnetz voraus. In diesem Modus dient nicht das mobile System, sondern der Foreign Agent als Tunnelendpunkt. Die Care-of-Adresse ist also eine dem Foreign Agent zugeordnete IP-Adresse. IP-Pakete, die vom Foreign Agent über den Tunnel empfangen werden, werden von ihm an das mobile System ausgeliefert. Da das mobile System und der Foreign Agent im gleichen Subnetz angesiedelt sind, werden die Pakete vom Foreign Agent zum mobilen System nicht geroutet, sondern mittels Schicht 2 Adressierung an das mobile System gesendet. Aus diesem Grunde können IP-Pakete – trotz nicht zum Subnetz passender Routing-Präfixes – an die permanente Adresse des mobilen Systems übertragen werden. Der wesentliche Vorteil des Foreign-Agent-Modus ist darin zu sehen, daß nicht für jedes unterstützte mobile System eine zusätzliche IP-Adresse notwendig ist. Unter dem Aspekt der Verknappung der IPv4-Adressen ist dieser Modus zu bevorzugen. Da weiterhin IP-Pakete nur bis zum Foreign Agent, aber nicht über die drahtlose Teilstrecke getunnelt werden, sind die Bandbreitenanforderungen über dieser Teilstrecke geringer als beim Colocated-Modus.

2.2.3 Protokollfunktionen

2.2.3.1 Agent Discovery

Das Agent Discovery erfüllt im Rahmen von Mobile IP drei Aufgaben. Zum einen wird es vom mobilen System dazu genutzt zu erkennen, ob es sich aktuell im Heimatsubnetz oder in einem fremden Subnetz befindet. Darüber hinaus kann das mobile System mit Hilfe des Agent Discoverys feststellen, ob ein Subnetzwechsel erfolgt ist oder nicht. Weiterhin wird das Agent Discovery im Foreign-Agent-Modus dazu benutzt, mobile Systeme über die IP-Adresse des Foreign Agents zu informieren, die als Care-of-Adresse zu verwenden ist.

Protokollablauf des Agent Discoverys
Es werden zwei verschiedene Arten des Agent Discoverys unterstützt. Bei beiden Varianten wird ein sogenanntes *Agent Advertisement* vom Mobility Agent, d.h. vom Home Agent oder vom Foreign Agent, ausgesandt. Die Varianten unterscheiden sich darin, wodurch das Aussenden eines Agent Advertisements veranlaßt wird:

- periodische Übertragung
  Agenten senden bei dieser Variante periodisch Agent Advertisements. Adressiert werden diese Advertisements entweder an die Multicast-Adresse 224.0.0.1 oder an die Limited-Broadcast-Adresse 255.255.255.255. Generell werden Advertisement nur in das Subnetz gesendet, für das ein Agent als Mobility Agent fungiert. Insbesondere werden die Advertisements nicht in andere Subnetze weitergeleitet.

- Übertragung nach expliziter Anforderung
  Alternativ zur periodischen Übertragung kann ein Agent Advertisement auch explizit von einem mobilen System angefordert werden. Ein mobiles System verwendet hierzu eine *Agent-Solicitation*-Nachricht. Diese Nachricht wird an die Multicast-Adresse 224.0.0.2 oder die Limited-Broadcast-Adresse 255.255.255.255 gesendet. Ein Mobility Agent antwortet nach Empfang eines Agent Solicitation mit einem Agent Advertisement.

Hat ein mobiles System das Subnetz gewechselt und ist im neuen Subnetz ein Mobility Agent verfügbar, so macht der beschriebene Ablauf Agent Advertisements zur Auswertung beim mobilen System verfügbar. Sind mehrere Mobility Agents innerhalb eines Subnetzes verfügbar, kann das mobile Endsystem aus diesen einen auswählen.

Nachrichten für das Agent Discovery
Die Übertragung von Agent-Discovery-Nachrichten erfolgt in Mobile IP unter Zuhilfenahme des ICMP-Router-Discovery-Protokolls [Dee91]. Diese Vorgehensweise ist naheliegend, da für ein Endsystem der Vorgang der Bestimmung des nächsten Routers mittels des *Router Discoverys* dem Vorgang der Ermittlung eines Mobility Agents nach einem Subnetzwechsel mittels des Agent Discoverys ähnlich ist.

Die Agent-Advertisement-Nachrichten werden in Erweiterungen kodiert, die an ICMP-Router-Discovery-Pakete angehängt werden. Drei verschiedene Erweiterungen sind in Mobile IP definiert: Die *Agent-Advertisement-Erweiterung*, die *Präfix-Längen-Erweiterung* zur Festlegung der Länge des Routing-Präfixes einer Care-of-Adresse und die *Padding-Erweiterung*. Die beiden letztgenannten Erweiterungen sind in [Per98b] im Detail beschrieben. Auf sie wird nicht weiter eingegangen, da sie für die vorliegende Arbeit nicht von Bedeutung sind. Das Format einer Agent-Advertisements-Erweiterung ist im Detail in Anhang A.1.1.1 dargestellt. Die wesentliche in der Agent-Advertisement-Erweiterung kodierte Information ist die Liste der Care-of-Adressen von Agenten, die innerhalb des Subnetzes die Rolle eines Mobility Agents übernehmen können. Darüber hinaus vermerkt ein Foreign Agent die jeweils von ihm unterstützten Operationsmodi in der Agent-Advertisements-Erweiterung.

Für Agent-Solicitation-Nachrichten ist in Mobile IP keine Erweiterung definiert. Stattdessen werden ICMP-Router-Solicitations gesendet, um Mobility Agents zu veranlassen, mit Agent Advertisements zu antworten.

Erkennen eines Subnetzwechsels
Ein mobiles System wertet es als einen Hinweis auf einen Subnetzwechsel, falls es von einem Foreign Agent, der bisher die Mobilitätsunterstützung realisiert und von dem es bisher Agent Advertisements empfangen hat, keine Advertisements mehr erhält. Das Ausbleiben von Advertisements ist allerdings kein hinreichendes Kriterium für einen Subnetzwechsel. Fällt ein für ein mobiles System verantwortlicher Mobility Agent aus und sind im gleichen Subnetz weitere Mobility Agents vorhanden, so kann einer dieser Agents die Mobilitätsunterstützung übernehmen. In diesem Fall liegt ein Wechsel des Agents aber kein Subnetzwechsel vor. Obwohl lediglich ein Wechsel des Foreign Agents stattgefunden hat, ist der Protokollablauf identisch zum Protokollablauf nach einem Subnetzwechsel. In Mobile IP wird der Wechsel des Foreign Agents innerhalb eines Subnetzes auf einen Subnetzwechsel abgebildet.

Jedes Agent Advertisement hat lediglich eine in der Agent-Advertisement-Erweiterung kodierte *Lebensdauer*. Läuft diese Lebensdauer ab, bevor ein nachfolgendes Advertisement vom gleichen Agent mit einer neuen Lebensdauer eintrifft, so wird vom mobilen System der zugehörige Foreign Agent als nicht mehr erreichbar angesehen und die Ermittlung eines neuen Foreign Agents als notwendig erachtet. Um im Falle vereinzelter Verluste von Agent Advertisements nicht sofort die Suche nach einem neuen Foreign Agent zu starten, wird in der Mobile IP Spezifikation vorgeschlagen, die in der Agent-Advertisement-Erweiterung kodierte Lebensdauer dreimal so groß wie die Zeitdauer zwischen zwei aufeinanderfolgenden Advertisements zu wählen.

Läuft die Lebensdauer eines Advertisements des Mobility Agents ab, der aktuell für die Mobilitätsunterstützung verantwortlich ist, so bestimmt ein mobiles System zunächst ein Advertisement, dessen Lebensdauer noch nicht abgelaufen ist. Hierzu werden Agent Advertisements von anderen Mobility Agents des Subnetzes ausgewertet und ggf. Agent Advertisements mittels eines Agent Solicitation angefordert. Anschließend erfolgt eine Registrierung durch die in Kapitel 2.2.3.2 beschriebenen Mechanismen.

Unterscheidung zwischen Heimatsubnetz und fremdem Subnetz
Die in einem mobilen System nach einem Subnetzwechsel vorzunehmenden Anpassungen sind davon abhängig, ob der Wechsel in ein fremdes Subnetz oder in das Heimatsubnetz erfolgt ist. Aus diesem Grunde muß das mobile System zunächst feststellen, ob es in das Heimatsubnetz oder in ein fremdes Subnetz gewechselt ist. Hierzu vergleicht es die IP-Absenderadresse des empfangenen Advertisements mit der Adresse des eigenen Home Agents. Sind beide identisch, so ist ein Wechsel in das Heimatsubnetz erfolgt.

Zuweisung einer Care-of-Adresse
Wechselt ein mobiles System in ein fremdes Subnetz, so muß ihm zunächst eine Care-of-Adresse zugewiesen werden. Mittels der Registrierung wird diese Care-of-Adresse dem Home Agent mitgeteilt.

2.2.3.2 Registrierung

Zweck der vom mobilen System veranlaßten Registrierung ist es, das mobile System bei den jeweiligen Mobility Agents bekannt zu machen. Dies ist erforderlich, damit die Mobility Agents über den Aufenthaltsort des mobilen Systems informiert sind und daraufhin ihre jeweilige

Aufgabe für die Mobilitätsunterstützung dieses mobilen Systems übernehmen können. Home Agents sind generell in den Prozeß der Registrierung involviert, Foreign Agents hingegen nur, falls das mobile System im Foreign-Agent-Modus operiert und falls der Wechsel in ein fremdes Subnetz erfolgt. Mobile IP Registrierungen werden zwischen dem mobilen System und dem Home Agent ausgetauscht. Im Falle des Einsatzes des Foreign-Agent-Modus stellt das in Unterkapitel 2.2.3.3 beschriebene Mobile IP Routing sicher, daß die Registrierungen über den Foreign Agent geroutet werden und dieser daraufhin die Mobilitätsunterstützung für das mobile System einrichten kann. Die *Lebensdauer einer Registrierung* beschränkt die Gültigkeit einer Registrierung. Eine Registrierung muß vor Ablauf dieser Lebensdauer durch eine erneute Registrierung aufgefrischt werden. Andernfalls wird die Mobilitätsunterstützung für das jeweilige mobile System beendet. Die Lebensdauer einer Registrierung ist nicht zu verwechseln mit der Lebensdauer eines Agent Advertisements.

Mobile IP Registrierungsnachrichten
Registrierungsanforderungen und *Registrierungsantworten* werden mittels UDP zwischen den mobilen Systemen und den Mobility Agents ausgetauscht. Da UDP nur einen unzuverlässigen Dienst zur Verfügung stellt, die Registrierung aber zuverlässig sein muß, sind in Mobile IP Mechanismen erforderlich, die die Zuverlässigkeit gewährleisten. Erreicht wird dies in Mobile IP durch die Verwendung des Request-Response-Paradigmas für die Registrierung: Bleibt auf eine vom mobilen System an den Home Agent gesendete Registrierungsanforderung die vom Home Agent generierte Registrierungsantwort aus, wiederholt das mobile System die Registrierungsanforderung.

Die Formate der vom mobilen System bzw. Home Agent generierten Registrierungsanforderung bzw. Registrierungsantwort sind in den Anhängen A.1.1.2 und A.1.1.3 dargestellt. Neben der im Nutzdatenfeld eines UDP-Pakets kodierten Registrierungsanforderung bzw. Registrierungsantwort muß auch die Quell- und Zieladresse im IP-Kopf definiert werden. Diesbezüglich unterscheiden sich der Foreign-Agent-Modus und der Colocated-Modus. Im folgenden wird darauf eingegangen.

Registrierung beim Home Agent (Foreign-Agent-Modus)
Im Foreign-Agent-Modus wählt das mobile System eine der im empfangenen Agent Advertisement aufgelisteten Care-of-Adressen aus und selektiert damit den zugehörigen Foreign Agent als den Foreign Agent, der die Mobilitätsunterstützung übernimmt. Die ausgewählte Care-of-Adresse wird in das Care-of-Adreßfeld der Registrierungsanforderung (siehe Abb. A.2 im Anhang) kopiert. Die Heimatadresse des mobilen Systems und die IP-Adresse des zugehörigen Home Agents sind dem mobilen System bekannt und werden in der Registrierungsanforderung kodiert. Als Lebensdauer wird das Maximum aus der vom mobilen System unterstützten Dauer und der im Agent Advertisement kodierten Lebensdauer eingetragen. Die in der Registrierungsantwort kodierte Lebensdauer kann vom Home Agent nach unten korrigiert werden. Die tatsächlich verwendete Lebensdauer kann das mobile System der Registrierungsantwort entnehmen und die Periode für die Erneuerung von Registrierungen darauf abstimmen.

Als Quelladresse wird im Kopf des IP-Pakets die permanente IP-Adresse des mobilen Systems verwandt. Die Registrierungsanforderung wird an den Foreign Agent adressiert. Seine IP-Adresse wird dem Agent Advertisement entnommen.

Empfängt ein Foreign Agent von einem mobilen System eine Registrierungsanforderung und kann der Agent für dieses mobile System als Foreign Agent fungieren, so leitet er sie an den Home Agent weiter. Als Zieladresse wird im IP-Paketkopf die Adresse des Home Agents eingetragen, die der Mobile IP Registrierungsanforderung entnommen werden kann. Absenderadresse ist die IP-Adresse des jeweiligen Netzwerkinterfaces des Foreign Agents.

Ein Home Agent überprüft bei Empfang einer Registrierungsanforderung zunächst die Gültigkeit der Anforderung und ob er das mobile System in der angeforderten Art und Weise unterstützen kann. Ist die in der Anforderung kodierte Lebensdauer von Null verschieden, wird die Care-of-Adresse der *Liste der Care-of-Adressen* hinzugefügt. Es werden dann alle an die permanente Adresse des mobilen Systems adressierten Pakete an die Care-of-Adresse getunnelt. Ist die in der Registrierungsanforderung kodierte Lebensdauer gleich Null, so liegt eine *Deregistrierung* vor. In diesem Fall wird die jeweilige Care-of-Adresse aus der Liste der bereits registrierten Care-of-Adressen entfernt. Mittels einer Registrierungsantwort (siehe Abb. A.3) informiert der Home Agent über den Erfolg bzw. Mißerfolg der Registrierungsanforderung. Die in der Registrierungsanforderung kodierte Heimatadresse des mobilen Systems und die IP-Adresse des Home Agents werden in die Registrierungsantwort kopiert. Die Lebensdauer wird vom Home Agent kleiner gleich dem in der Registrierungsanforderung spezifizierten Wert gewählt. Im IP-Paketkopf der Registrierungsantwort wird als Zieladresse die Quelladresse der Registrierungsanforderung und als Quelladresse die Zieladresse der Registrierungsanforderung verwandt.

Der Foreign Agent empfängt direkt vom Home Agent die Registrierungsantwort. Hat der Home Agent die Registrierung akzeptiert, so ist eine positive Lebensdauer in der Registrierungsantwort kodiert. Der Foreign Agent paßt nach Empfang der Registrierungsantwort den Timer an, der bei Ablauf die Mobilitätsunterstützung für das jeweilige mobile System beendet. Anschließend wird die Registrierungsantwort an das mobile System gesendet.

Das mobile System paßt im Falle einer akzeptierten Registrierung die verbleibende Lebensdauer der Registrierung dem Wert an, der in der Registrierungsantwort kodiert ist. Wird die Registrierung nicht akzeptiert, so wird eine erneute Registrierung – ggf. über einen anderen Foreign Agent – veranlaßt.

Registrierung beim Home Agent (Colocated-Modus)
Kommt der Colocated-Modus zum Einsatz, wird dem mobilen System zunächst mittels DHCP eine temporäre IP-Adresse zugewiesen, die als Care-of-Adresse zu verwenden ist. Im Vergleich zum Foreign-Agent-Modus ändert sich die Adressierung der Registrierungsanforderungen bzw. Registrierungsantworten. In der vom mobilen System gesendeten Registrierungsanforderung wird die Colocated-Care-of-Adresse als Quelladresse kodiert. Zieladresse ist die IP-Adresse des Home Agents. Da keine Advertisements eines Foreign Agents berücksichtigt werden müssen, kann seitens des mobilen Systems die in der Registrierungsanforderung kodierte Lebensdauer frei ohne Vorgaben eines Foreign Agents gewählt werden. Die Bearbeitung einer empfangenen Registrierungsanforderung beim Home Agent erfolgt analog zu der den Foreign-Agent-Modus nutzenden Variante von Mobile IP. Die zur Registrierungsanforderung gehörige Registrierungsantwort wird direkt an das mobile System gesendet. Quelladresse bzw. Zieladresse der Registrierungsanforderung werden als Ziel- bzw. Quelladresse der Registrierungsantwort genutzt.

Deregistrierung beim Home Agent
Eine Lebensdauer Null in einer Registrierungsanforderung (siehe Abb. A.3) kennzeichnet diese als Deregistrierung. Den Empfang einer Deregistrierung bestätigt der Home Agent ebenfalls mit einer Registrierungsantwort. Zweck einer Deregistrierung ist es, den Home Agent darüber zu informieren, daß das Weiterleiten der an ein mobiles System adressierten IP-Pakete zu einer bestimmten Care-of-Adresse nicht mehr erforderlich ist. Es gibt zwei verschiedene Gründe für eine Deregistrierung: Zum einen wird eine Deregistrierung aller Care-of-Adressen eines mobilen Systems vorgenommen, falls das mobile System in sein Heimatsubnetz zurückgekehrt ist und somit keine Weiterleitung in andere Subnetze mehr erforderlich ist. Zum anderen kann ein mobiles System auch gezielt einzelne Care-of-Adressen deregistrieren. Erkennt ein mobiles System beispielsweise, daß Agent Advertisements von einem bestimmten Foreign Agent ausbleiben, so kann es die diesem Foreign Agent zugeordnete Care-of-Adresse beim Home Agent deregistrieren.

Ein Home Agent, der eine Registrierungsanforderung mit einer Lebensdauer Null empfängt, macht seine weiteren Aktionen von der in der Registrierungsanforderung kodierten Care-of-Adresse und der kodierten Heimatadresse abhängig. Sind beide identisch, ist das mobile System in sein Heimatsubnetz gewechselt. Da eine Mobilitätsunterstützung seitens des Home Agents nicht mehr erforderlich ist, werden *alle* registrierten Care-of-Adressen des mobilen Systems gelöscht und das Mobile IP Routing dahingehend modifiziert, daß an das mobile System adressierte Pakete nicht mehr über den Home Agent weitergeleitet, sondern direkt an das mobile System ausgeliefert werden. Sind die kodierte Care-of-Adresse und die Heimatadresse nicht identisch, wird lediglich die *eine* spezifizierte Care-of-Adresse deregistriert. Das Routing für die verbleibenden Care-of-Adressen bleibt in diesem Fall unverändert.

Wiederholung von Registrierungsanforderungen
Es gibt in Mobile IP zwei verschiedene Gründe, die eine Wiederholung einer Registrierungsanforderung veranlassen können:

- Ausbleiben einer Registrierungsantwort und
- Periodische Reregistrierung (wegen begrenzter Lebensdauer einer Registrierung).

Um das Ausbleiben einer Registrierungsantwort zu erkennen, erfolgt das Senden einer Registrierungsanforderung seitens eines mobilen Systems unter der Kontrolle eines Timers. Läuft dieser Timer ab, geht das mobile System davon aus, daß entweder die Registrierungsanforderung oder die Registrierungsantwort verloren gegangen ist, und veranlaßt eine erneute Registrierung.

Periodische Registrierungen sind notwendig, da Registrierungen auf den Mobility Agents und den mobilen Systemen nur eine begrenzte Lebensdauer haben, und daher regelmäßig durch erneute Registrierungen aufgefrischt werden müssen. Die maximale unterstütze Lebensdauer ist für Home Agents, Foreign Agents und mobile Systeme individuell konfigurierbar. In [GD96] wird beispielsweise defaultmäßig eine maximale Lebensdauer von 300 Sekunden verwendet. Damit eine nicht erfolgreiche Registrierung nicht sofort zur Beendigung der Mobilitätsunterstützung führt, sollte die Periode, in der Registrierungen wiederholt werden, ein Drittel der Lebensdauer einer Registrierung betragen. Auch das Fehlschlagen zweier aufeinanderfolgender Registrierungsversuche führt in dem Fall einer erfolgreichen nachfolgenden dritten Registrierung nicht zum Ende der Mobilitätsunterstützung.

Solange die Lebensdauer einer bestehenden Registrierung nicht abgelaufen ist, nutzt ein mobiles System die Care-of-Adresse, die es auch bei den vorangegangen Registrierungen eingesetzt hat. Obwohl ggf. mehrere verschiedene Agenten in einem Subnetz ihre Existenz mittels Advertisements ankündigen, kann somit sichergestellt werden, daß ein mobiles System nicht fortlaufend versucht, sich bei einem anderen Foreign Agent zu registrieren.

2.2.3.3 Mobile IP Routing

Die folgenden Ausführungen beziehen sich auf das Routing von Unicast-Paketen. Hinsichtlich des Routings von Broadcast- bzw. Multicast-Paketen sei auf [Per98b] verwiesen. In Mobile IP sind für das Routing der IP-Pakete in das Subnetz, über das das mobile System aktuell an das Internet angebunden ist, spezielle Mechanismen notwendig. Das in Unterkapitel 2.2.1 beschriebene Präfix-Routing routet an die permanente IP-Adresse eines mobilen Systems adressierte Pakete immer in das Heimatsubnetz dieses Systems. Um aber eine globale Mobilitätsunterstützung zu realisieren, müssen in Mobile IP ggf. IP-Pakete vom Home Agent in das fremde Subnetz weitergeleitet werden. Hierzu können die folgenden beiden Verfahren eingesetzt werden:

- Source Routing und
- Tunnel.

Beim Source Routing [Hui00] erfolgt die Routingentscheidung innerhalb eines Routers nicht auf Basis des Routing-Präfixes der Zieladresse. Stattdessen wird anhand einer im Kopf eines IP-Pakets kodierten Liste von IP-Adressen entschieden, an welche IP-Adresse, d.h. an welchen Router das Paket als nächstes zu senden ist. Indem im Home Agent die Care-Of-Adresse in diese Liste aufgenommen wird, läßt sich das Routing des IP-Pakets zu dieser Adresse erzwingen. Problematisch an diesem Lösungsansatz ist, daß das Source Routing in Routern teilweise ineffizient bzw. sogar fehlerhaft implementiert ist [Per98a].

Alternativ zum Source Routing kann ein *Tunnel*-Mechanismus für das Weiterleiten der IP-Pakete vom Home Agent in das fremde Subnetz eingesetzt werden. Pakete, die am Tunnelanfang in den Tunnel gesendet werden, werden zum Tunnelendpunkt transportiert. Für die Realisierung des Tunnel-Konzeptes ist keine spezielle Unterstützung in den IP-Routern erforderlich. Die Weiterleitung eines IP-Pakets zum Tunnelendpunkt wird – trotz Präfix-Routings innerhalb des Internets – erreicht, indem das IP-Paket modifiziert wird. Das modifizierte Paket wird durch das Präfix-Routing zum Tunnelendpunkt geroutet. Dort wird die Modifikation rückgängig gemacht. Drei Varianten der Modifikation der IP-Pakete werden in Mobile IP vorgeschlagen: Die *Minimale Einkapselung* [Per96c], die *Generic-Record-Einkapselung* [HLFT94] und die *IP-in-IP-Einkapselung* [Per96a]. Wegen der geringen Verbreitung der ersten beiden Varianten wird auf diese nicht weiter eingegangen. Die IP-in-IP-Einkapselung wird im folgenden kurz skizziert, da auch die im Rahmen der vorliegenden Arbeit entwickelte Fast-Forwarding-Erweiterung für Mobile IP diese nutzt.

IP-in-IP-Einkapselung
Bei der IP-in-IP-Einkapselung [Per96a] wird am Tunnelanfang ein kompletter, zusätzlicher IP-Paketkopf vor das zum Tunnelendpunkt weiterzuleitende IP-Paket gesetzt. Dieser zusätzliche

IP-Paketkopf wird als *äußerer Kopf* bezeichnet. Quell- bzw. Zieladresse sind die IP-Adressen des Tunnelanfangspunktes bzw. Tunnelendpunktes. Die IP-Adresse des Tunnelendpunktes erfährt der als Tunnelanfangspunkt fungierende Home Agent mittels der Mobile IP Registrierungsanforderung. Da im äußeren Kopf als Zieladresse die IP-Adresse des Tunnelendpunktes eingetragen ist, kann das Präfix-Routing die Pakete zum Tunnelendpunkt routen. Das innere IP-Paket wird im Nutzdatenfeld des äußeren IP-Pakets plaziert. Abb. 2.8 zeigt, wie IP-Pakete vom Festnetzrechner zum mobilen System mittels der IP-in-IP-Einkapselung übertragen werden. Die im inneren bzw. äußeren IP-Paketkopf kodierten IP-Adressen sind ebenfalls mit aufgenommen. Vom mobilen System gesendete Pakete werden vom Foreign Agent direkt zum Festnetzrechner übertragen. Das beschriebene Routing wird auch als Dreiecksrouting bezeichnet.

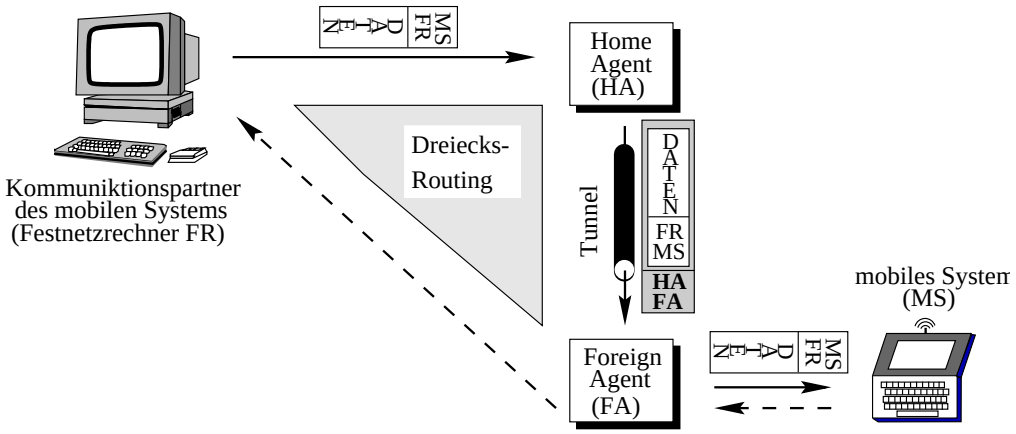


Abbildung 2.8: Dreiecksrouting von IP-Paketen in Mobile IP

Damit ein mobiles System IP-Pakete senden kann, muß es seinen Default Router kennen. Welcher Default Router im Heimatsubnetz bzw. in einem fremden Subnetz zu verwenden ist, wird im folgenden diskutiert.

Default Router mobiler Systeme
Ein mobiles System, das in seinem Heimatsubnetz an das Internet angebunden ist, erfährt durch ICMP-Nachrichten von seinem Default Router. In einem fremden Subnetz verwendet es im Fall des Foreign-Agent-Modus den Foreign Agent als Default Router und im Fall des Colocated-Modus einen durch ICMP-Nachrichten bekannt gemachten Router als Default Router.

Verwendung des Address Resolution Protocols (ARP) im Kontext von Mobile IP
Da an die permanente IP-Adresse eines mobilen Systems gesendete IP-Pakete nicht an den Home Agent des Heimatsubnetzes adressiert sind, kann dieser sie nicht ohne spezielle Maßnahmen empfangen. Der Home Agent verwendet den sogenannten *Proxy-Arp*-Mechanismus [Pos84], damit an die permanente IP-Adresse eines mobilen Systems adressierte IP-Pakete zum Home Agent gesendet werden [Per98a]. Der Home Agent antwortet im Heimatsubnetz auf ARP-Anfragen zur Ermittlung der Schicht 2 Adresse eines mobilen Systems mit seiner eigenen Schicht 2 Adresse. Somit wird erreicht, daß eigentlich für das mobile System bestimmte IP-Pakete an den Home Agent gesendet werden. Damit nach einem Wechsel eines mobilen Systems zurück in sein Heimatsubnetz die IP-Pakete nicht mehr zum Home Agent gesendet werden, wird der *gratuitous-ARP*-Mechanismus [Pos84] eingesetzt.

2.2.4 Weitergehende Entwicklungen

Die Ausführungen in den vorangegangenen Abschnitten bezogen sich auf die Mechanismen von Mobile IP wie sie in RFC 2002 [Per96b] spezifiziert sind. Weitergehende bzw. neuere Entwicklungen werden im folgenden nur kurz angesprochen, aber nicht im Detail betrachtet.

Um an ein mobiles System adressierte IP-Pakete nicht über den Home Agent, sondern direkt an das mobile System zu routen, kann die sogenannte *Routenoptimierung* eingesetzt werden. Hierzu wird der Kommunikationspartner des mobilen Systems über die temporäre Adresse des mobilen Systems informiert, so daß er IP-Pakete direkt an diese Adresse tunneln kann [PJ00].

In Mobile IP werden Registrierungen immer beim unter Umständen weit entfernten Home Agent vorgenommen. In [GJP00], [Per96d], [MHW+99], [FC98], [CL98] werden Hierarchien von Foreign Agents vorgeschlagen. Eine Registrierung eines mobilen Systems erfolgt dann nicht mehr beim weit entfernten Home Agent, sondern bei einem Foreign Agent in der lokalen Umgebung. An das mobile System adressierte IP-Pakete werden weiterhin an diesen Foreign Agent gesendet. Lediglich das Routing von diesem Agent zum mobilen System muß modifiziert werden. Insgesamt lassen sich mit diesem Verfahren schneller und damit auch häufiger Registrierungen nach Subnetzwechseln realisieren.

Eine weitere Entwicklung, die nicht unerwähnt bleiben soll, ist das in RFC 3024 beschriebene Reverse Tunneling [Mon01]. Beim Reverse Tunneling werden vom mobilen System gesendete Pakete zurück zum Home Agent getunnelt und von dort weiter geroutet, d.h. es liegt kein Dreiecksrouting mehr vor. Von einem mobilen System aus einem fremden Subnetz gesendete IP-Pakete tragen dann nicht die permanente IP-Adresse des mobilen Systems als Absenderadresse, sondern eine zu dem Subnetz "passende" IP-Adresse, d.h. eine Adresse mit korrektem Routing-Präfix. Das Reverse Tunneling wird erforderlich, falls Router zur Vermeidung von Denial-of-Service-Attacken [FS98] IP-Pakete mit nicht passender Absenderadresse verwerfen. Weiterhin ermöglicht es das Reverse Tunneling dem mobilen System, auch in fremden Subnetzen Multicast-Gruppen beizutreten.

Die Mobilitätsunterstützung in IPv6 ist in [JP00] beschrieben. Da das in der vorliegenden Arbeit entwickelte OMIT-Konzept auf der mittels Mobile IP für IPv4 realisierten globalen Mobilitätsunterstützung aufsetzt, wird auf IPv6 nicht detaillierter eingegangen. Es wird lediglich in Kapitel 6 kurz skizziert, inwieweit IPv6 und das OMIT-Konzept grundsätzlich vereinbar sind.

2.2.5 Beispiele verfügbarer Implementierungen

Während die Unterstützung portabler Systeme durch die Integration von DHCP in die verfügbaren Betriebssysteme bereits Einzug erhalten hat, ist die Mobilitätsunterstützung mittels Mobile IP derzeit nicht in diese Betriebssysteme integriert. Einen Überblick über aktuell verfügbare, zumeist im forschungsnahen Umfeld entstandene Implementierungen von Mobile IP gibt Tabelle 2.3. Eine Auflistung, die auch Implementierungen der Mobilitätsunterstützung für IPv6 enthält, ist beispielsweise in [Dar00] zu finden.

Die in die Tabelle 2.3 aufgenommenen Zeitpunkte der letzten Version der jeweiligen Implementierung (Stand Januar 2001) zeigen, daß abgesehen von der Dynamics-HUT Implementierung [AFH+99] und der Implementierung der Stanford University [BZCS96] die letzten

Projekt	Institution	Betriebssystem	Version vom	**K**ern/ **U**ser **S**pace	Route Opt.	Rev. Tunnel	Hierarchie
CMU Monarch Project [MJ97]	Carnegie Mellon University	FreeBSD	1/98	K/US	x	–	–
Secure Mobile Networking [BBM97]	Portland State University and MIT	FreeBSD	12/99	K/US	–	–	–
Linux Mobile-IP [GD96]	State Univ. of New York, Binghamton	Linux	3/98	US	–	–	–
Mobile IP At NUS [Cho96]	National Univ. of Singapore	Linux	10/99	K	x	x	–
MosquitoNet [BZCS96]	Stanford University	Linux	8/00	K/US	-	x	–
Mobile IP for Solaris/Linux [Gup98]	SUN	Solaris, Linux	12/98	US	x	–	–
Dynamics-HUT Mobile IP [AFH+99]	Helsinki Univ. of Technology	Linux	11/00	US	x	x	x
RoamIn-NT [FLM98]	GMD Fokus and Univ. of Bucharest	Wind. NT 4.0	unbekannt	US	x	–	–

Tabelle 2.3: Beispiele verfügbarer Mobile IP Implementierungen

Releases länger zurückliegen. Die Dynamics-HUT Implementierung entwickelt sich weiter, da Konzepte für die Unterstützung von Hierarchien von Foreign Agents in sie integriert werden. Bei der Version 8/00 von der Stanford University handelt es sich hingegen nicht um eine Weiterentwicklung, sondern lediglich um ein Anpassung der Vorgängerversion auf Linux 2.2. Linux Mobile-IP [GD96] zählt zu den sehr früh verfügbaren Mobile IP Implementierungen für Linux, wird aber inzwischen nicht mehr weiter entwickelt. Eine Mobile IP Implementierung für Solaris und Linux [Gup98] wird von dem Entwickler, der zuvor maßgeblich an der Entwicklung von Linux Mobile-IP beteiligt war, bei der Firma SUN betreut. Die an der University of Singapore entstandene Mobile IP Implementierung [Cho96] ist komplett im Linux-Betriebssystemkern realisiert. Sie hat somit den Nachteil einer sehr großen Abhängigkeit von der Version des jeweiligen Linux Kerns.

Die Implementierungen der Carnegie Mellon University [MJ97] und der Portland State University [BBM97] sind für das Betriebssystem FreeBSD konzipiert. Allerdings umfaßt die Implementierung der Portland State University lediglich die Funktionalität im mobilen System. Mobility Agents sind nicht realisiert.

Die aufgelisteten Implementierungen nehmen für sich in Anspruch, konform zu RFC 2002 zu sein. Inwieweit sie die Routenoptimierung, Reverse Tunneling bzw. Hierarchien von Agenten realisieren und ob die Realisierung im Kern bzw. im User Space erfolgt, kann ebenfalls Tabelle 2.3 entnommen werden. Interoperabilitätstests und Untersuchungen der Performance sind für einige der aufgelisteten Implementierungen in [FHMR98] zu finden.

2.3 Das Transportprotokoll TCP

Aufgabe des Transmission Control Protocols (TCP) ist es, einen zuverlässigen Datendienst zwischen dem Sender und dem Empfänger zur Verfügung zu stellen. Übertragungsfehler müssen vom Transportprotokoll erkannt und korrigiert werden. Den Transportprotokollmechanismen, die für die Fehlererkennung und die Fehlerkorrektur verantwortlich sind, kommt insbesondere im Fall drahtlos angeschlossener mobiler Systeme auf Grund der dann häufiger auftretenden Übertragungsfehler eine größere Bedeutung zu als im Fall der drahtgebundenen Kommunikation. Eine detaillierte Beschreibung der TCP-Protokollmechanismen ist in [Ste94] zu finden, die Implementierung betreffende Aspekte in [WS95].

2.3.1 Protokollmechanismen von TCP

Der von einer sendenden Anwendung an TCP übergebene *Nutzdatenstrom* wird von TCP in einzelne *Segmente* unterteilt. Diese Segmente werden mittels *Nutzdatenpaketen* von der TCP-Instanz des Senders zur TCP-Instanz des Empfängers übertragen. Mittels *Bestätigungen* informiert der Empfänger den Sender bezüglich korrekt empfangener Nutzdaten. Nutzdatenpakete werden unter der Kontrolle eines Timers vom Sender übertragen. Empfängt der Sender vor Ablauf des Timers keine Bestätigung, so veranlaßt er eine erneute Übertragung des Nutzdatenpakets. Die Mechanismen der Fehlererkennung und der Fehlerkorrektur werden in Unterkapitel 2.3.1.1 beschrieben.

Um trotz Reihenfolgevertauschung von TCP-Nutzdatenpaketen die Nutzdaten in der gleichen Reihenfolge, in der sie beim Sender an TCP übergeben wurden, beim Empfänger an die Anwendung ausliefern zu können, verwendet TCP *Sequenznummern*. TCP-Sequenznummern sind Byte-basiert. Die Bytes des Nutzdatenstromes werden fortlaufend numeriert. Im Sequenznummernfeld eines TCP-Nutzdatenpakets wird die Nummer des ersten in diesem Paket enthaltenen Nutzdatenbytes kodiert. Mittels der Sequenznummern kann beim Empfänger eine vollständige und reihenfolgetreue Auslieferung der Nutzdaten an die Anwendung realisiert werden.

In TCP-Instanzen wird ein Sendepuffer und ein Empfangspuffer verwaltet. Senderseitig werden Nutzdaten für ggf. notwendige Übertragungswiederholungen im *Sendepuffer* aufbewahrt. Empfängerseitig werden sie im *Empfangspuffer* zwischengespeichert, bis sie eine die Transportverbindung nutzende Anwendung aus diesem entnimmt. Da die empfangende Transportinstanz nur über einen Empfangspuffer beschränkter Größe verfügt, besteht die Gefahr eines Überlaufens des Empfangspuffers, falls die sendende Transportinstanz nicht rechtzeitig von der Übertragung weiterer Segmente absieht. Die in Kapitel 2.3.1.2 beschriebene *Flußkontrolle* von TCP verhindert Empfangspufferüberläufe. Um im Falle einer Überlastung einzelner Teilstrecken innerhalb des Netzwerkes die seitens des Senders an das Netzwerk übergebene Datenmenge zu reduzieren, kommt die in Kapitel 2.3.1.3 vorgestellte *Lastkontrolle* von TCP zum Einsatz.

2.3.1.1 Fehlererkennung und Fehlerkorrektur

Bitfehler innerhalb eines TCP-Pakets werden anhand einer Prüfsumme erkannt. Fehlerhafte Pakete werden verworfen, d.h. ein Bitfehler innerhalb eines Pakets wird auf einen Paketverlust

abgebildet. Duplikate von Nutzdatenpaketen werden anhand der Sequenznummer erkannt und beim Empfänger verworfen. Reihenfolgevertauschungen werden ebenfalls beim Empfänger anhand der Sequenznummern festgestellt und korrigiert. Die Erkennung und Behebung von Paketverlusten ist komplexer als die Korrektur der zuvor aufgeführten Fehlerarten. Sie wird im folgenden detaillierter beschrieben.

Bestätigungen

Um seitens des Senders die erneute Übertragung von Paketen veranlassen zu können, muß dieser vom Empfänger Feedback hinsichtlich erfolgreich bzw. nicht erfolgreich übertragener Pakete erhalten. Durch eine im TCP-Paketkopf kodierte sogenannte *Bestätigungs-Sequenznummer* wird der Sender über korrekt empfangene Nutzdatenpakete informiert. Die Bestätigungs-Sequenznummer ist die Sequenznummer des ersten Nutzdatenbytes (d.h. mit der niedrigsten Sequenznummer), das noch *nicht* korrekt vom Empfänger erhalten wurde. Sogenannte *kumulative Bestätigungen* werden mittels der Bestätigungs-Sequenznummer realisiert. Eine kumulative Bestätigungs-Sequenznummer *Ack* bedeutet, daß alle Nutzdatenbytes n mit $n < Ack$ korrekt empfangen wurden. Dies bedeutet andererseits aber auch, daß im Falle eines nicht korrekt empfangenen Nutzdatenbytes die Nutzdaten mit höherer Sequenznummer nicht bestätigt werden können, da andernfalls die nicht korrekt empfangenen Bytes des Nutzdatenstromes mit bestätigt werden würden. Soll, obwohl das Nutzdatenbyte mit der Sequenznummer l noch nicht korrekt empfangen wurde, ein Nutzdatenbyte n mit $n > l$ bestätigt werden, so kann hierzu eine sogenannte *selektive Bestätigung* genutzt werden. Mittels einer selektiven Bestätigung kann ein Sender über den korrekten Empfang einer Folge von mehreren Nutzdatenbytes, die unter Umständen in mehreren Paketen zum Empfänger übertragen wurden, unterrichtet werden. Selektive Bestätigungen sind im Detail in [JBB92] beschrieben.

Der Zeitpunkt, zu dem vom Empfänger ein Bestätigungspaket generiert wird, ist davon abhängig, welches Segment aus dem Nutzdatenstrom vom Empfänger empfangen wurde. Kann der Empfänger nach Erhalt der Nutzdaten kumulativ eine höhere Sequenznummer als vor Erhalt dieser Daten bestätigen und hat er nicht bereits zuvor Nutzdaten mit einer höheren Sequenznummer empfangen, so kann er die Generierung der Bestätigung bis zu 0.2 Sekunden verzögern. In allen anderen Fällen muß unmittelbar nach Erhalt des Nutzdatenpakets eine Bestätigung gesendet werden, in der unter Umständen wiederholt die gleiche Bestätigungs-Sequenznummer kodiert ist. Wird die Bestätigung nicht sofort gesendet, so spricht man von einer *verzögerten Bestätigung*.

Das Verfahren der Bestätigung in TCP wird in Abb. 2.9 anhand verschiedener Weg-Zeit-Diagramme verdeutlicht, die sich hinsichtlich Paketverlusten und Reihenfolgevertauschungen von Paketen unterscheiden. Die Sequenznummern (Seq) der 512 Nutzdatenbytes umfassenden Pakete und die in Bestätigungspaketen kodierten kumulativen Bestätigungs-Sequenznummern (Ack) sind in der Abbildung dargestellt. Da die im nächsten Abschnitt beschriebenen Übertragungswiederholungen ebenfalls anhand Abb. 2.9 erläutert werden, sind die Übertragungswiederholungen und die verwendeten Timer in diese Abbildung mit aufgenommen.

In Abb. 2.9a erhält der Empfänger die Nutzdatenpakete reihenfolgetreu und ohne Paketverluste. Die Pakete mit den Sequenznummern 1, 2049, 2561 werden einzeln bestätigt. Eine einzelne verzögerte Bestätigung, die kumulative mehrere Nutzdatenpakete bestätigt, ist ebenfalls möglich. In Abb. 2.9a erfolgt die Bestätigung der Sequenznummern 513 bis 2048 verzögert. Welche Bestätigungsstrategie angewandt wird, obliegt dem Empfänger.

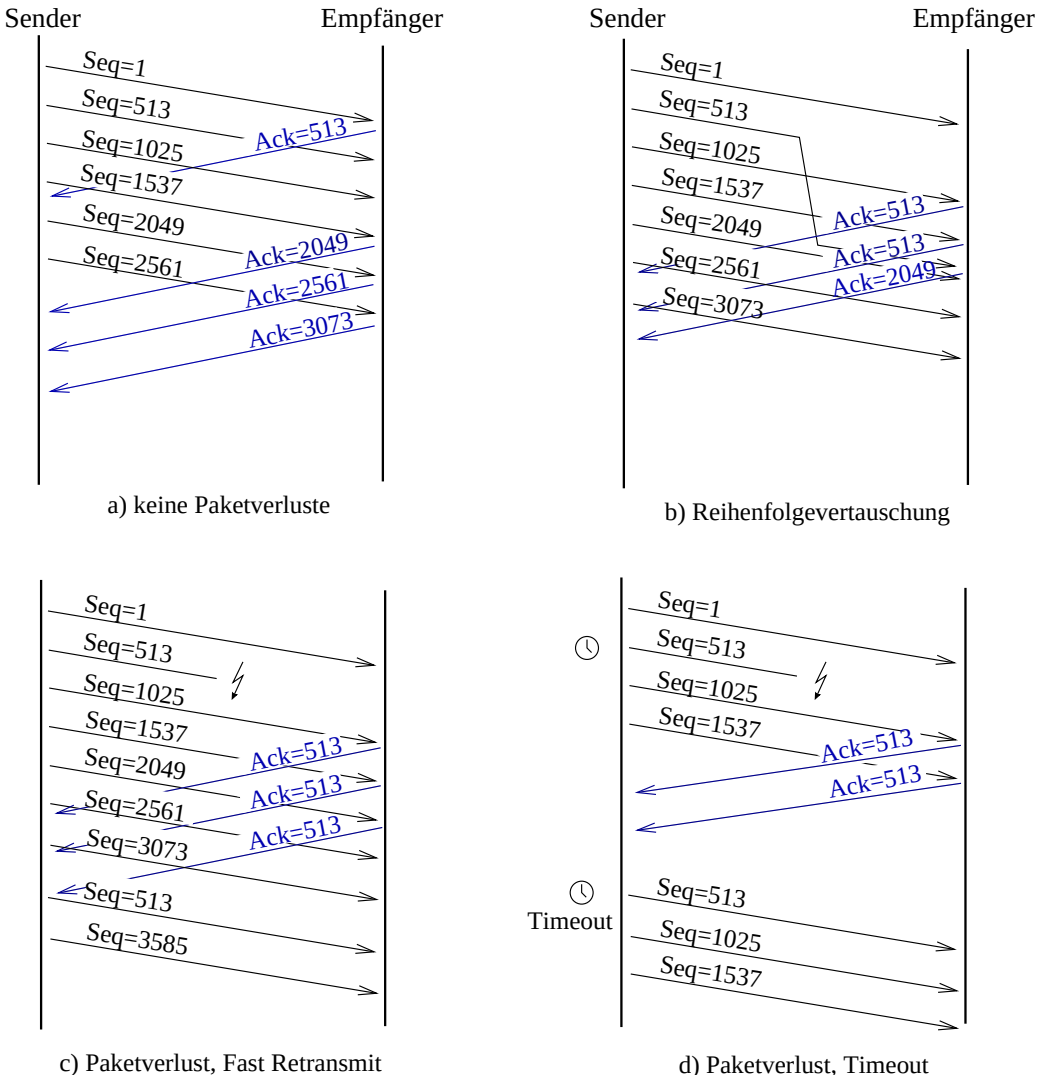


Abbildung 2.9: Bestätigungsstrategien und Fehlerkorrektur in TCP

In Abb. 2.9b liegt eine Reihenfolgevertauschung von Nutzdatenpaketen vor. Für das Paket mit der Sequenznummer 1 wird keine Bestätigung gesendet, da der Empfänger diese verzögern will. Nach Empfang des Pakets mit der Sequenznummer 1025 muß er ohne Verzögerung eine Bestätigung generieren, da er eine Lücke im Datenstrom erkannt hat. Bei Empfang der Pakete mit den Sequenznummern 1025, 1537 kann jeweils lediglich die Bestätigungs-Sequenznummer $Ack = 513$ verwendet werden. Erst nach Empfang des Nutzdatenpakets mit der Sequenznummer 513 erfolgt eine kumulative Bestätigung bis zur Sequenznummer 2048.

In Abb. 2.9c ist der Verlust des Pakets mit der Sequenznummer 513 dargestellt. Für alle mit höherer Sequenznummer beim Empfänger eintreffenden Pakete wird ohne Verzögerung ein Bestätigungspaket gesendet. Da das Paket mit der Sequenznummer 513 noch nicht eingetroffen ist, kann lediglich die Bestätigungs-Sequenznummer $Ack = 513$ verwendet werden. Auf die durch den *Fast-Retransmit-Mechanismus* veranlaßte Übertragungswiederholung wird erst bei der Diskussion der Übertragungswiederholungen eingegangen.

Abb. 2.9d zeigt ebenfalls den Verlust eines Pakets. Allerdings werden im dargestellten Szenario lediglich zwei weitere Nutzdatenpakete nach dem verlorengegangenen Paket vom

Sender übertragen. Für diese Pakete werden vom Empfänger Bestätigungen mit der Bestätigungs-Sequenznummer $Ack = 513$ generiert. Die durch einen *Timeout* veranlaßte Übertragungswiederholung wird im nachfolgenden Abschnitt beschrieben.

Erkennen der Notwendigkeit einer Übertragungswiederholung
Damit ein Sender die erneute Übertragung eines Pakets veranlassen kann, muß er ein Indiz für die Notwendigkeit einer Paketwiederholung haben. Hierzu werden beim Sender die eintreffenden Bestätigungspakete ausgewertet. Die im folgenden aufgeführten Ereignisse liefern den Hinweis für die Notwendigkeit einer Wiederholung eines Nutzdatenpakets:

- Empfang von Bestätigungsduplikaten und
- Ausbleiben von Bestätigungen (Timeout).

Als *Bestätigungsduplikat* wird eine Bestätigung bezeichnet, die eine Sequenznummer bestätigt, die bereits in einem vorangegangenen Bestätigungspaket bestätigt wurde. Wie in Abb 2.9 dargestellt, werden Duplikate dann generiert, wenn Nutzdatenpakete nicht reihenfolgetreu beim Empfänger eintreffen. Empfängt der Sender drei Bestätigungspakete, die alle die gleiche Sequenznummer bestätigen, so nimmt er an, daß nicht eine Reihenfolgevertauschung der Nutzdatenpakete, sondern ein Paketverlust die Ursache für die Bestätigungsduplikate ist. Ein Hinweis auf den Verlust mehrerer Nutzdatenpakete kann aus dem Empfang von Bestätigungsduplikaten nicht abgeleitet werden. Aus diesem Grunde wird genau ein Nutzdatenpaket wiederholt. Dieser Mechanismus wird als *Fast Retransmit* bezeichnet. In Abb. 2.9b und Abb. 2.9d erfolgt keine Paketwiederholung, da lediglich zwei Bestätigungspakete mit identischer Bestätigungs-Sequenznummer empfangen werden. In Abb. 2.9c erfolgt hingegen eine Wiederholung des Pakets mit der Sequenznummer 513.

Auch das Ausbleiben einer Bestätigung für ein Nutzdatenpaket ist ein Indiz für den Verlust des zugehörigen Nutzdatenpakets. Um den Verlust eines Nutzdatenpakets oder der zugehörigen Bestätigung zu erkennen, bedient sich TCP eines Timermechanismus. Zeitgleich zum Senden eines Nutzdatenpakets wird ein Timer mit einem geeignet gewählten Timeoutwert gestartet. Der Timeoutwert richtet sich hierbei nach der geschätzten Paketumlaufzeit. Beim Empfang eines Bestätigungspakets mit der zugehörigen Sequenznummer wird der Timer gestoppt. Ein *Timeout* ist ein Indiz, aber kein sicheres Kriterium für einen Paketverlust, da beispielsweise auch durch Überlast innerhalb des Netzwerkes bedingte Verzögerungen zu einem Timeout führen können. Trotzdem veranlaßt TCP nach einem Timeout eine Übertragungswiederholung des jeweiligen Pakets. Darüber hinaus geht TCP davon aus, daß auch die Pakete nach dem Paket, für das der Timeout erfolgt ist, nicht korrekt zum Empfänger übertragen wurden und wiederholt diese ebenfalls.

In Abb. 2.9d ist ein Szenario dargestellt, das zu einem Timeout führt. Da der Sender nach dem verlorengegangenen Paket mit der Sequenznummer 513 nur noch zwei weitere Pakete sendet, werden genau zwei Bestätigungsduplikate generiert. Eine Übertragungswiederholung wird nicht veranlaßt, da hierzu drei Bestätigungsduplikate erforderlich wären. Stattdessen erfolgt erst nach dem Timeout die erneute Übertragung des Pakets mit der Sequenznummer 513 und der nachfolgenden Pakete.

Timer
Die Wahl des Timeoutwertes ist bei TCP von zentraler Bedeutung. Wird der Timeoutwert zu klein gewählt, so werden unnötigerweise Übertragungswiederholungen und weitere Maßnahmen veranlaßt, obwohl kurze Zeit später das jeweilige Bestätigungspaket eintrifft und diese Maßnahmen nicht erforderlich gewesen wären. Wird andererseits ein zu großer Timeoutwert gewählt, so wird – falls die Übertragungswiederholung nicht durch Bestätigungsduplikate veranlaßt wird – die Übertragungswiederholung unnötig lange verzögert. Grundproblem bei der Wahl des Timeoutwertes ist, daß der Timeoutwert die für die Übertragung des Nutzdatenpakets und der zugehörigen Bestätigung erforderliche Zeit reflektieren muß, diese aber a priori nicht bekannt ist. Die folgenden beiden Mechanismen verwendet TCP für die Bestimmung der zu verwendenden Timeoutwerte:

- Schätzung der Paketumlaufzeit auf Basis gemessener Umlaufzeiten und
- Exponentieller Backoff-Mechanismus.

Um die Paketumlaufzeiten zu ermitteln, bestimmt TCP die Zeitdifferenz zwischen dem Senden eines Pakets mit einer bestimmten Sequenznummer und einem Paket, das diese Sequenznummer bestätigt, oder im Falle einer kumulativen Bestätigung, diese Sequenznummer mit bestätigt. [Ste94] beschreibt das Verfahren, wie aus einem gewichteten Mittel aus dem alten Initialisierungswert und dem neuen Meßwert unter zusätzlicher Berücksichtigung der Schwankungen der gemessenen Umlaufzeiten der neue zu verwendende Timeoutwert berechnet wird.

Für Pakete, die wiederholt gesendet werden, ist die Bestimmung der Paketumlaufzeit nicht eindeutig möglich, da das Bestätigungspaket nicht genau einer von ggf. mehreren Übertragungswiederholungen eines Nutzdatenpakets zugeordnet werden kann. Diese Problematik ist in Abb. 2.10a dargestellt. Da das Paket mit der Sequenznummer 513 im Netz verzögert wird, werden nach Ablauf des Timers vom Sender dieses und die nachfolgenden Pakete erneut übertragen. Sowohl für den ersten Sendeversuch als auch für den zweiten Sendeversuch wird eine Bestätigung generiert. Empfängt der Sender diese Bestätigungen, ist für ihn nicht erkennbar, ob er für die Bestimmung der Paketumlaufzeit die Zeitdifferenz zum ersten oder zum zweiten Sendeversuch heranziehen muß. Der sogenannte *Karn-Algorithmus* [KP87] spezifiziert, daß im Falle wiederholter Pakete keine Messungen der Paketumlaufzeit und keine neue Bestimmung eines Timeoutwertes erfolgen.

Mittels sogenannter *Zeitstempel* kann auch für wiederholt gesendete Pakete die Paketumlaufzeit bestimmt werden. Grundidee hierbei ist es, den Absendezeitpunkt in einer TCP-Option an das Nutzdatenpaket anzuhängen und beim Empfänger in das Bestätigungspaket zu kopieren [Ste94]. Der Sender kann aus dem Zeitpunkt des Empfangs der Bestätigung und dem im Paket kodierten Sendezeitpunkt die Paketumlaufzeit eindeutig bestimmen. In Abb. 2.10b können zum Zeitpunkt t_4 für das wiederholte Paket mit der Sequenznummer 513 die Paketumlaufzeiten bestimmt werden.

Während ohne die Zeitstempel-Option immer nur für das aktuell unter der Kontrolle des Timers gesendete Paket eine Messung der Paketumlaufzeit möglich ist, kann mittels der Zeitstempel-Option für jedes Paket die Paketumlaufzeit bestimmt werden. Diese Option bietet somit den Vorteil einer größeren Anzahl von Meßwerten. Insbesondere im Falle häufiger und starker Schwankungen der Paketumlaufzeiten ist dies von Vorteil.

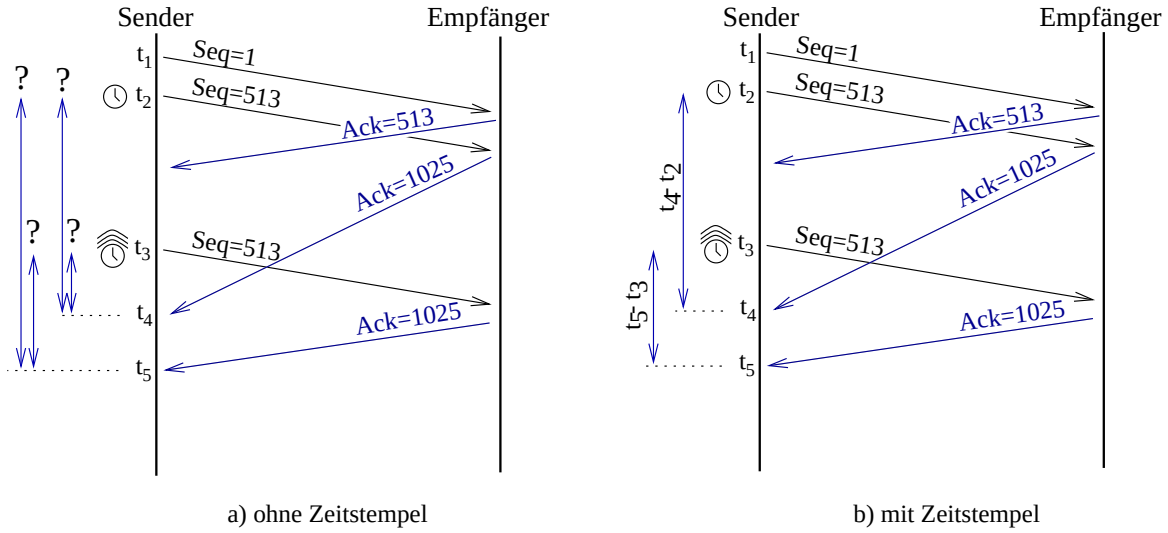


Abbildung 2.10: Die Zeitstempel-Option

Tritt für ein unter Kontrolle eines Timers gesendetes Paket ein Timeout ein, so wird der zu verwendende Timeoutwert gemäß des *exponentiellen Backoff*-Mechanismus verdoppelt und dieser verdoppelte Timeoutwert für die erneute Übertragung des Pakets verwendet. Tritt mehrfach hintereinander ein Timeout ein, so wird auch der Timer mehrfach hintereinander verdoppelt. Der Grund für dieses Verhalten ist darin zu sehen, daß TCP nicht sicher davon ausgehen kann, den Timer groß genug gewählt zu haben. Vorsichtshalber wird deshalb bei jedem Timeout der Initialisierungswert verdoppelt und solange dieser Wert verwendet, bis eine neue aktuelle Messung der Paketumlaufzeit vorliegt und diese als Basis für die Bestimmung eines geeigneten neuen Timeoutwertes verwendet werden kann.

Wiederholungsstrategien
TCP nutzt zwei verschiedene Strategien der Übertragungswiederholung. Erfolgt eine Übertragungswiederholung nach einem *Timeout*, werden das Paket, für das der Timeout erfolgt ist, und alle nachfolgenden, bereits gesendeten Nutzdatenpakete gemäß der *Go-Back-N*-Strategie wiederholt. Ist der Empfang des dritten Bestätigungsduplikates der Anlaß für die Wiederholung, wird nur ein Nutzdatenpaket wiederholt. Dieser Mechanismus wird als *Fast Retransmit* bezeichnet.

2.3.1.2 Flußkontrolle

Um das Überlaufen des in seiner Größe beschränkten Empfangspuffers einer TCP-Instanz zu vermeiden, muß sichergestellt sein, daß der Sender nicht mehr Nutzdaten sendet, als der Empfänger in seinem Puffer aufnehmen kann. Dies ist die Aufgabe der Flußkontrolle. TCP benutzt hierfür ein *Flußkontrollfenster*, das sich mit dem Fortgang der Nutzdatenübertragung verändert und aus diesem Grunde als *gleitendes Flußkontrollfenster* bezeichnet wird. Es ist durch seine untere und obere Grenze bestimmt. Die Sequenznummern, die im Kontext der Übertragungswiederholung und Bestätigung von Nutzdaten verwendet werden, werden auch dazu genutzt, diese beiden Grenzen festzulegen.

Im Verlauf der Übertragung der Nutzdaten bewegt sich das Flußkontrollfenster hin zu größeren Sequenznummern. Mittels der Bestätigungspakete informiert der Empfänger den Sender über die Bestätigungs-Sequenznummer und die sogenannte *Flußkontrollfenstergröße*. Die Bestätigungs-Sequenznummer legt die untere Grenze des Flußkontrollfensters, die Summe aus dieser und der Flußkontrollfenstergröße die obere Sequenznummer fest. Der Sender überträgt keine Nutzdaten mit einer über diese obere Grenze hinausgehenden Sequenznummer.

In Abb. 2.11 ist ein Ausschnitt aus einem zu übertragenden Nutzdatenstrom zuzüglich der aktuellen Position des Flußkontrollfensters dargestellt. Auf der linken Seite ist die im letzten empfangenen Bestätigungspaket kodierte Bestätigungs-Sequenznummer und die Flußkontrollfenstergröße aufgeführt.

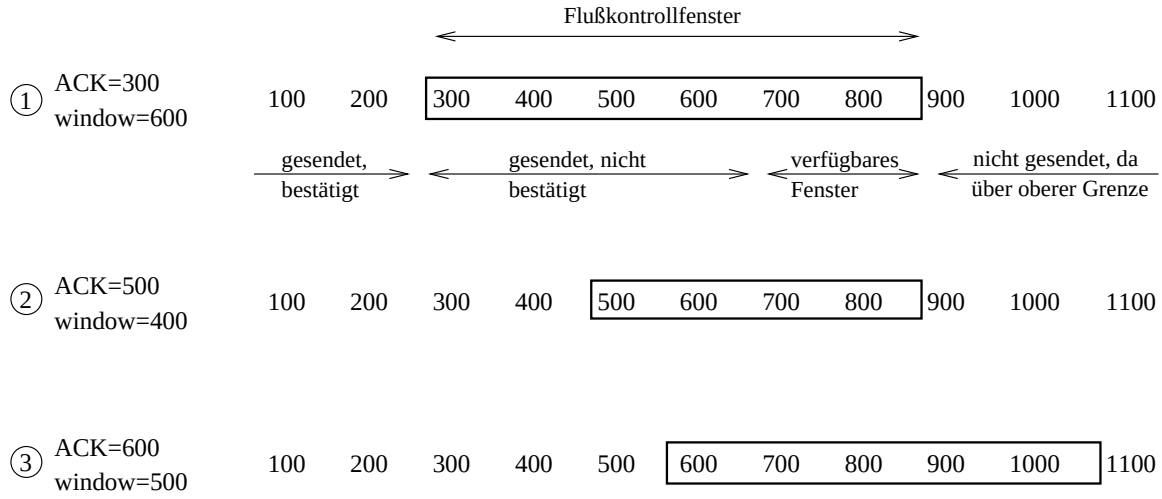


Abbildung 2.11: Flußkontrolle mittels gleitendem Flußkontrollfenster

Mittels der Bestätigungs-Sequenznummer 300 und einer Fenstergröße von 600 informiert der Empfänger den Sender, daß im Empfangspuffer Platz für die Nutzdaten mit der Sequenznummer 300 bis 899 verfügbar ist. Diese Nutzdaten dürfen vom Sender gesendet und im Falle von Übertragungswiederholungen auch mehrmals gesendet werden. Die zweite dargestellte Bestätigung ist ein Beispiel dafür, wie der Empfänger zwar Nutzdaten bestätigt, aber keinen zusätzlichen Sendekredit gewährt. Mittels der dritten Bestätigung werden 100 Bytes Nutzdaten neu bestätigt und zugleich auch die obere Grenze des Flußkontrollfensters um 200 Bytes verschoben.

Einen Sonderfall stellt die Flußkontrollfenstergröße Null dar. Empfängt der Sender ein Bestätigungspaket mit der Flußkontrollfenstergröße Null, so wechselt er in den sogenannten *Persist-Modus*. In diesem Modus werden keine Nutzdatenpakete mehr gesendet. Darüber hinaus werden auch die Timer angehalten, so daß keine Timeouts mehr erfolgen. Sobald der Empfänger das Flußkontrollfenster erneut öffnet, wird die Kommunikation wieder aufgenommen.

2.3.1.3 Lastkontrolle

Die Lastkontrolle von TCP [APS99] wird mittels eines *Lastkontrollfensters* realisiert. Das Lastkontrollfenster bestimmt, bis zu welcher Obergrenze Nutzdatenbytes gesendet werden dürfen. Während die Flußkontrolle den Empfänger vor Pufferüberläufen schützt, ist es die

Aufgabe der Lastkontrolle, Überlastsituationen innerhalb des Netzwerkes zu vermeiden bzw. aufzulösen. Die Größe und Veränderung des Flußkontrollfensters wird vom Empfänger gesteuert, die des Lastkontrollfensters hingegen vom Sender. Wie auch bei der Flußkontrolle werden Sequenznummern dazu genutzt, die Grenzen des Lastkontrollfensters festzulegen. Die Summe aus der höchsten bestätigten Sequenznummer und der Größe des Lastkontrollfensters bestimmt die obere Grenze des Lastkontrollfensters. Der Sender darf nur Nutzdatenpakete übertragen, die weder die obere Grenze des Flußkontrollfensters noch die obere Grenze des Lastkontrollfensters überschreiten.

Explizite Feedback Signale, denen der Sender die Notwendigkeit einer Vergrößerung oder Verkleinerung des Lastkontrollfensters entnehmen kann, stehen TCP nicht zur Verfügung. TCP kann lediglich implizite Signale nutzen. Empfängt der Sender Bestätigungspakete vom Empfänger, so ist das ein Indiz dafür, daß Pakete der Verbindung transportiert werden und keine Überlast vorliegt. Der Sender vergrößert daraufhin das Lastkontrollfenster. Diagnostiziert TCP anhand eines Timeouts oder anhand von Bestätigungsduplikaten einen vermeintlichen Paketverlust, wird dies als Indiz für eine Überlast gewertet und daraufhin die Lastkontrollfenstergröße reduziert und somit eine sogenannte *Lastreduktion* vorgenommen. Hinsichtlich der Verfahren für die Anpassung des Lastkontrollfensters muß unterschieden werden, inwieweit ihr Einsatz in TCP zwingend vorgeschrieben bzw. optional ist. Die ersten beiden der im folgenden aufgelisteten Verfahren müssen in TCP implementiert sein, das dritte ist optional:

- Slow Start,
- Congestion Avoidance und
- Fast Recovery (optional).

Der *Slow Start* kommt beim Start einer Verbindung und im Falle der Notwendigkeit einer drastischen Lastreduktion zum Einsatz. Das Ziel von *Congestion Avoidance* ist es, die Last so zu regulieren, daß die Last zwar langsam bis zur Überlastung erhöht wird, bei Überschreiten der Engpaßkapazität aber nur eine geringfügige Überlastung die Folge ist. *Fast Recovery* wird nach einer Übertragungswiederholung mittels Fast Retransmit eingesetzt.

Der sogenannte *Slow-Start-Grenzwert* regelt, wann das Slow-Start-Verfahren bzw. das Congestion-Avoidance-Verfahren die Last adaptiert. Ab dem Zeitpunkt einer durch einen Timeout oder durch Bestätigungsduplikate veranlaßten Übertragungswiederholung wird die Hälfte der Anzahl der gesendeten, aber nicht bestätigten Nutzdatenbytes als neuer Grenzwert verwendet.

Slow Start
Das Konzept des Slow Starts ist es, mit einer sehr geringen Last zu starten, aber zügig, d.h. exponentiell, die Last zu erhöhen. Hierzu wird das Lastkontrollfenster, das zu Beginn eines Slow Starts auf die Größe eines Segments gesetzt wird, beim Empfang jedes Bestätigungspakets um die Größe eines Segments vergrößert. Dies ergibt insgesamt ein exponentielles Öffnen des Lastkontrollfensters in der Phase des Slow Starts. Ein Slow Start wird nicht nur beim Start einer Verbindung durchgeführt. Nach einem Timeout wird ebenfalls ein Slow Start vorgenommen, d.h. das Lastkontrollfenster wird auf die Größe eines Segments gesetzt und anschließend wieder exponentiell vergrößert. Überschreitet die Größe des Lastkontrollfensters den *Slow-Start-Grenzwert*, adaptiert nicht mehr das Slow-Start-Verfahren, sondern das Congestion-Avoidance-Verfahren die Größe des Lastkontrollfensters.

Congestion Avoidance
Der Congestion-Avoidance-Algorithmus vergrößert jede Paketumlaufzeit das Lastkontrollfenster um die Größe eines Segments und erhöht somit die Last linear. Da im Vergleich zum Slow-Start-Verfahren die Last wesentlich langsamer erhöht wird, ist im Fall einer Überlastung das Ausmaß der Überlast wesentlich geringer. Erhöht der Sender jede Paketumlaufzeit die während dieser Zeit gesendete Datenmenge um ein Paket, und nimmt man eine konstante Engpaßkapazität an, hat die Erhöhung den Verlust von genau einem Paket zur Folge. Ist das Fast-Retransmit-Verfahren nicht implementiert, ist ein Timeout mit anschließendem Slow Start die Folge. Wird der Paketverlust durch Bestätigungsduplikate erkannt und anschließend mittels Fast Retransmit eine Wiederholung veranlaßt, übernimmt – sofern implementiert – das Fast Recovery die Lastkontrolle.

Fast Recovery
Nach einer Übertragungswiederholung mittels Fast Retransmit wird die Summe aus dem neu bestimmten Slow-Start-Grenzwert und der dreifachen Segmentgröße als neue Lastkontrollfenstergröße verwendet. Weiterhin wird für jedes empfangene Bestätigungsduplikat das Lastkontrollfenster um die Größe eines Segments vergrößert. Empfängt der Sender ein Bestätigungspaket, das bisher noch nicht bestätigte Nutzdaten bestätigt, wird der aktuelle Slow-Start-Grenzwert als neue Lastkontrollfenstergröße verwendet und das Fast Recovery beendet. Anschließend wird das Lastkontrollfenster mittels des Congestion-Avoidance-Verfahrens adaptiert.

Lastkontrollverfahren in einem beispielhaften Szenario
Die Veränderung des Lastkontrollfensters während des Slow Starts, der Congestion Avoidance und des Fast Recoverys und die Anpassung des Slow-Start-Grenzwertes sind in Abb. 2.12 dargestellt. Es wird von einer Segmentgröße von 1000 Bytes ausgegangen.

Auf Grund eines Timeouts wird zum Zeitpunkt 0 das Lastkontrollfenster auf ein Segment und der Slow-Start-Grenzwert auf 16000 Byte reduziert. Bis zum Erreichen dieses Grenzwerts wird vom Slow-Start-Verfahren das Lastkontrollfenster exponentiell geöffnet. Bei Erreichen des Grenzwertes zum Zeitpunkt 4 übernimmt das Congestion-Avoidance-Verfahren die Lastkontrolle. Es erhöht die Last lediglich um 1000 Bytes pro Paketumlaufzeit. Zum Zeitpunkt 7 wird ein Paketverlust festgestellt und eine Übertragungswiederholung veranlaßt. Da zu diesem Zeitpunkt 18000 Bytes gesendeter Nutzdaten unbestätigt sind, verwendet der Sender 18000/2 Bytes als neuen Slow-Start-Grenzwert. Wie das Lastkontrollfenster nach der Übertragungswiederholung adaptiert wird, ist abhängig davon, ob die Wiederholung nach einem Timeout (Variante 1 in Abb. 2.12) oder durch Fast Retransmit (Variante 2 in Abb. 2.12) erfolgt.

Im Falle eines Timeouts wird – analog zur Übertragungswiederholung zum Zeitpunkt 0 – ein Slow Start vorgenommen und anschließend die Last durch das Congestion-Avoidance-Verfahren reguliert. Wird mittels Fast Retransmit wiederholt, ist ab dem Zeitpunkt 7 das Fast-Recovery-Verfahren für die Lastkontrolle verantwortlich. Die Größe des Lastkontrollfensters beträgt $\textit{Slow-Start-Grenzwert} + 3 * 1000 = 12000$ Bytes und wird bei Empfang der 4 Bestätigungsduplikate jeweils erhöht. Zum Zeitpunkt 8 werden bisher nicht bestätigte Nutzdaten bestätigt. Aus diesem Grunde übernimmt ab diesem Zeitpunkt das Congestion-Avoidance-Verfahren die Lastkontrolle.

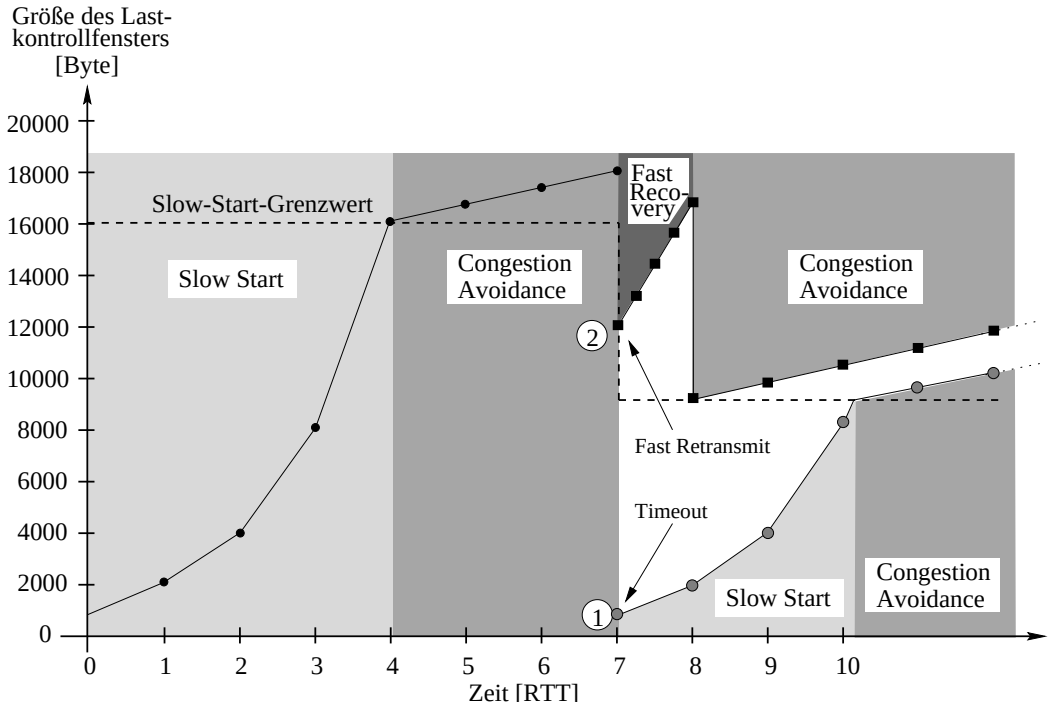


Abbildung 2.12: Veränderung des Lastkontrollfensters

Wesentlicher Nachteil der Strategie, Paketverluste implizit als Indiz für eine Überlast zu verwenden, ist, daß nicht nur durch Pufferüberläufe in Routern bedingte Paketverluste als Überlast interpretiert werden. Wird ein Paket durch einen Bitfehler verfälscht, so wird es nach Überprüfung verworfen. Sobald der Sender den Paketverlust erkennt, reduziert er, allerdings unnötigerweise, die Last. Insbesondere im Umfeld der drahtlosen Übertragung mit häufigeren, aber nicht unbedingt durch Pufferüberläufe bedingten Paketverlusten führt dies zu unnötigen Lastreduktionen und sich daraus ergebenden drastischen Durchsatzeinbußen.

2.3.2 TCP in drahtlosen Umgebungen

TCP wurde ursprünglich für den Betrieb über drahtgebundenen Übertragungskanälen konzipiert. Es wurde von Übertragungskanälen mit weitgehend konstanten Bitfehlerraten ausgegangen, die kleiner als 10^{-6} sind. Höhere Fehlerraten, wie sie für drahtlose Netze typisch sind, wurden nicht gezielt adressiert. Auch zur Behandlung von Unterbrechungen des Übertragungskanals sind in TCP keine speziellen Mechanismen vorgesehen, da diese Art von Unterbrechungen zum Zeitpunkt der Entwicklung von TCP nicht als typisch angesehen wurde. Zum damaligen Zeitpunkt wurde von etablierten Routen, stationären Endsystemen, die mangels Ortsveränderungen nur selten Routenanpassung erforderlich machten, und einem zuverlässigen, dauerhaft verfügbaren Übertragungskanal ausgegangen. Der Verzicht auf Mechanismen, die Unterbrechungen des Übertragungskanals oder höhere Bitfehlerraten adressieren, war somit naheliegend.

Hinsichtlich der Übertragungseigenschaften liegt im Falle von Endsystemen, die drahtlos angeschlossen und mobil sind, eine signifikant andere Situation vor. Die funkbasierte Übertragung ist fehleranfälliger und hat eine höhere Bitfehlerrate als die drahtgebundene Kommunikation zur Folge. Darüber hinaus unterliegt die Bitfehlerrate stärkeren Schwankungen.

Eine Ursache hierfür ist die Tatsache, daß sich ein Funkkanal nicht wie ein Kabel gegen Störeinflüsse abschirmen läßt. Bedingt durch Ortswechsel eines mobilen Systems oder sich im Ausbreitungspfad des Funksignals bewegender Gegenstände kann ein mobiles System mit höheren Bitfehlerraten konfrontiert werden (siehe Kapitel 2.1.4).

	drahtgebundene Übertragung	drahtlose Übertragung
längere Unterbrechungen	selten	häufig
Bitfehlerrate	$10^{-6} - 10^{-12}$	$10^{-3} - 10^{-6}$
Schwankungen der Bitfehlerrate	gering	stark

Tabelle 2.4: Übertragungseigenschaften

Tabelle 2.4 verdeutlicht die unterschiedlichen Übertragungseigenschaften der drahtgebundenen bzw. der funkbasierten Übertragung. Auf Grund der signifikant verschiedenen Übertragungseigenschaften stellt sich die Frage, inwieweit das ursprünglich für die Kommunikation über drahtgebundenen Medien entwickelte Transportprotokoll TCP auch über fehleranfälligen Funkkanälen eingesetzt werden kann.

2.3.2.1 Auswirkungen von Bitfehlern

Da höhere Bitfehlerraten in drahtlosen Netzen keine Ausnahmesituationen darstellen, sondern zumindest zeitweise im regulären Betrieb auftreten, ist zu untersuchen, wie Protokolle höherer Schichten sich im Falle dieser Fehlerraten verhalten. Von besonderer Bedeutung ist hierbei die Transportschicht, da die Übertragungsfehler von ihr korrigiert werden müssen. Den im folgenden aufgelisteten Aspekten kommt somit eine größere Bedeutung zu:

- Verzögerung bis zur Übertragungswiederholung
  Im Falle häufig notwendiger Übertragungswiederholungen muß darauf geachtet werden, daß diese Wiederholungen von TCP möglichst schnell veranlaßt werden.

- Effizienz der Übertragungswiederholung
  Ist lediglich die Übertragung einzelner Pakete und nicht die Übertragung von Paketen eines kompletten Flußkontrollfenster erfolglos, so ist die Übertragungswiederholung mittels Go-Back-N nicht effizient. Auf Grund ggf. unnötig wiederholter Pakete werden Übertragungsressourcen verschwendet.

- Auswirkungen auf die Lastkontrolle
  Wie in Kapitel 2.3.1.3 beschrieben, wertet TCP Paketverluste als Indiz für eine Überlastsituation. Paketverluste auf Grund von Übertragungsfehlern werden somit – allerdings fälschlicherweise – als Überlast interpretiert. Das Verhalten des Slow-Start-Mechanismus und des Congestion-Avoidance-Verfahrens muß aus diesem Grunde im Kontext von durch Übertragungsfehler bedingten Paketverlusten untersucht werden.

Wie sich Paketverluste, die nicht durch Pufferüberläufe während einer Überlastsituation bedingt sind, auf TCP auswirken, ist abhängig davon, wie häufig derartige Verluste auftreten.

Einzelner Paketverlust pro Paketumlaufzeit
Werden nach dem Nutzdatenpaket, das nicht erfolgreich zum Empfänger übertragen wurde, mindestens drei Nutzdatenpakete erfolgreich übertragen, so kann der Sender anhand der vom Empfänger generierten Bestätigungsduplikate den Paketverlust vermuten und mittels Fast Retransmit die Wiederholung dieses Pakets veranlassen. Die Übertragungswiederholung erfolgt schnell und ist effizient, da sie unmittelbar erfolgt und nur das eine nicht korrekt übertragene Paket wiederholt wird. Allerdings wird auch das Lastkontrollfenster verkleinert. Abb. 2.13 zeigt die Entwicklung der Lastkontrollfenstergröße. Bis zum Zeitpunkt 8 hat das Congestion-Avoidance-Verfahren ein lineares Anwachsen der Größe zur Folge. Ohne Lastreduktion würde das Lastkontrollfenster zwar weiter wachsen, ein größerer Durchsatz würde sich aber nicht ergeben, da das Flußkontrollfenster den begrenzenden Faktor darstellt. Im Zeitraum 8 bis 9 wird das Lastkontrollfenster unter der Kontrolle von Fast Recovery adaptiert. Zum Zeitpunkt 9 wird der aktuelle Slow-Start-Grenzwert als neue Lastkontrollfenstergröße verwendet. Anschließend übernimmt das Congestion-Avoidance-Verfahren die Lastkontrolle. Der grau markierte Bereich verdeutlicht die unnötige Durchsatzeinbuße.

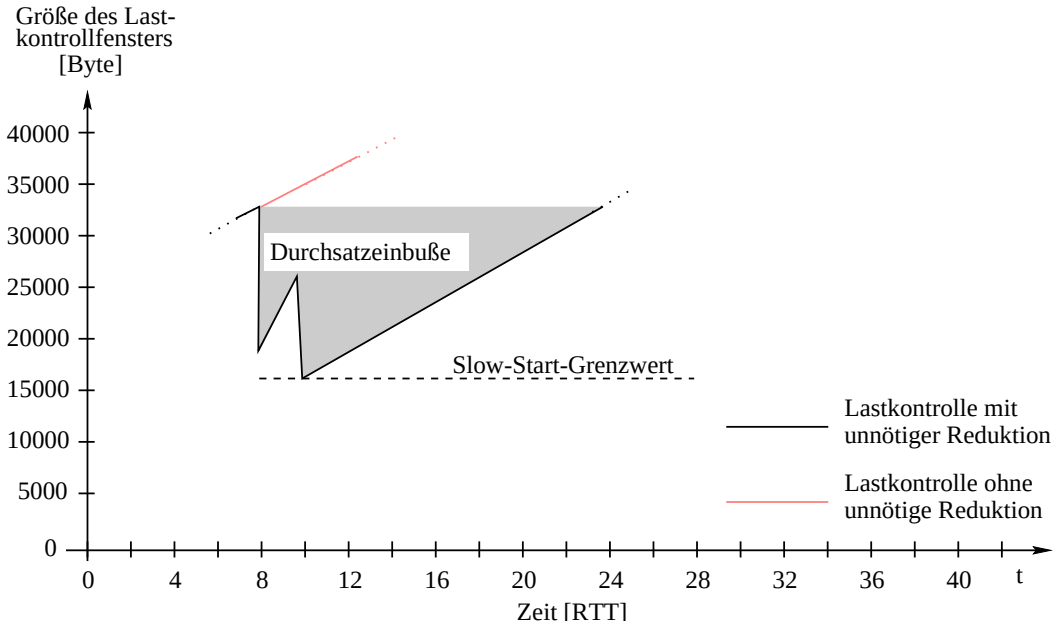


Abbildung 2.13: Durchsatzeinbußen nach einem einzelnem Paketverlust

Mehrere Paketverluste pro Paketumlaufzeit
Treten mehrere Paketverluste innerhalb einer Paketumlaufzeit auf, so kann nur der erste dieser Verluste mittels Fast Retransmit und anschließendem Fast Recovery korrigiert werden. Der Verlust des zweiten Pakets wird erst anhand des Timeouts des zugehörigen Timers erkannt. Wieviel Zeit bis zur Übertragungswiederholung verstreicht, ist damit davon abhängig, wie präzise die Paketumlaufzeit geschätzt wurde. Auch Implementierungsdetails des TCP-Protokolls spielen hierbei eine Rolle. BSD verwendet beispielsweise einen Timer mit einer Granularität von 500 ms und einem Minimalwert von 500 ms, die Granularität des Linux Timers beträgt hingegen 10 ms und hat einen Minimalwert von 200 ms [BBD+99]. Aus diesem Grunde wird in der Regel von Linux eine Übertragungswiederholung schneller veranlaßt als von BSD. Nichtsdestotrotz verstreicht bis zur Übertragungswiederholung nach einem Timeout

mehr Zeit als bis zur durch Fast Retransmit veranlaßten Wiederholung. Eine signifikante und unnötig lange Verzögerung ergibt sich auch dann, falls unnötigerweise ein zu großer Initialisierungswert für den Timer gewählt wird. Dies ist insbesondere dann der Fall, wenn nach einem Timeout für die Übertragung des wiederholten Pakets gemäß des exponentiellen Backoff-Mechanismus ein verdoppelter Timerinitialisierungswert verwendet wird. Da der Karn-Algorithmus vorgibt, daß für wiederholte Pakete keine Messungen der Paketumlaufzeit vorgenommen werden, wird während mehrerer Paketumlaufzeiten dieser zu pessimistisch gewählte verdoppelte Timeoutwert verwendet. Treten in dieser Zeit erneut Paketverluste auf, die nur durch einen Timeout erkannt werden können, so wird die Übertragungswiederholung unnötig lange verzögert. Abb. 2.14 verdeutlicht die beschriebene Situation. Die zwischen Sender und Empfänger gesendeten Pakete und die Veränderung des verwendeten Timeoutwertes sind dargestellt.

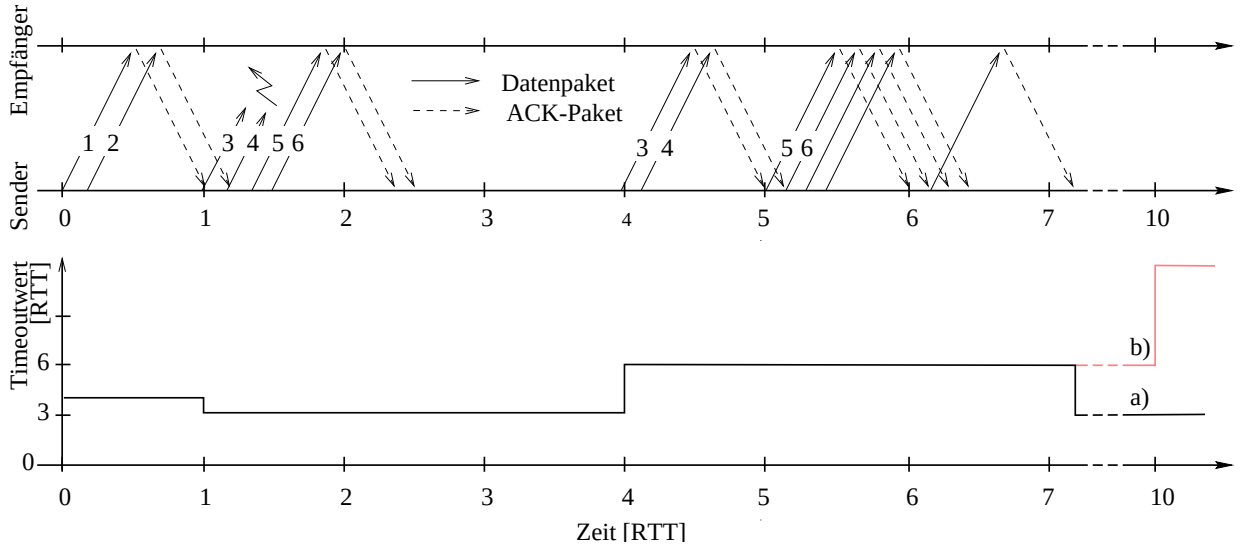


Abbildung 2.14: Verzögerung von Übertragungswiederholungen

Zum Zeitpunkt 1 liegt eine neue RTT Messung vor und es wird ein neuer zu verwendender Timeoutwert von 3 berechnet. Die Pakete 3 und 4 gehen verloren. Da der Sender nicht mindestens 3 Bestätigungsduplikate empfängt, kann er kein Fast Retransmit veranlassen. Zum Zeitpunkt 4 läuft der Timer ab, und es werden die Pakete 3 und 4 wiederholt. Die Pakete 5 und 6 werden hingegen noch nicht wiederholt, da das Lastkontrollfenster die Übertragung beschränkt. Für die Übertragung wird gemäß des exponentiellen Backoff-Mechanismus ein Timeout von 6 verwendet. Erst zum Zeitpunkt 7.2 empfängt der Sender die Bestätigung für ein Paket, das er nicht wiederholt hat. Somit kann eindeutig die RTT für dieses Paket bestimmt und auch ein neuer Timeoutwert errechnet werden (Fall a). Angenommen, eines der Pakete 3, 4 könnte nicht erfolgreich übertragen werden, so würde zum Zeitpunkt 10 erneut ein Timeout erfolgen und der zu verwendende Timeoutwert nochmals verdoppelt werden (Fall b).

Diese pessimistischen Timeoutwerte verzögern in dem Falle, daß erst durch einen Timeout eine Übertragungswiederholung veranlaßt wird, diese unnötig lange. Je länger diese pessimistischen Timeoutwerte verwendet werden, um so größer ist die Wahrscheinlichkeit, daß während dieser Zeit ein Paketverlust eintritt und keine Kommunikation bis zum Ablaufen dieses pessimistisch gewählten Timers erfolgt. Im dargestellten Szenario werden lediglich die Pakete 3-6, d.h. 4 Pakete, wiederholt und anschließend Pakete, die erstmalig übertragen werden, gesen-

det. Muß ggf. ein komplettes Flußkontrollfenster wiederholt werden (Go-Back-N), so dauert es länger, bis ein noch nicht gesendetes Paket übertragen wird, für das eine Messung der Paketumlaufzeit vorgenommen werden und statt des ggf. mehrfach verdoppelten Timeoutwertes ein realistischerer verwendet werden kann.

Bei einem Timeout wird generell das Lastkontrollfenster auf seine minimale Größe reduziert. Wird ein Paket auf Grund eines Bitfehlers nicht korrekt übertragen, ist diese Lastreduktion nach dem Timeout nicht sinnvoll. Die Entwicklung des Lastkontrollfensters ist in Abb. 2.15 dargestellt.

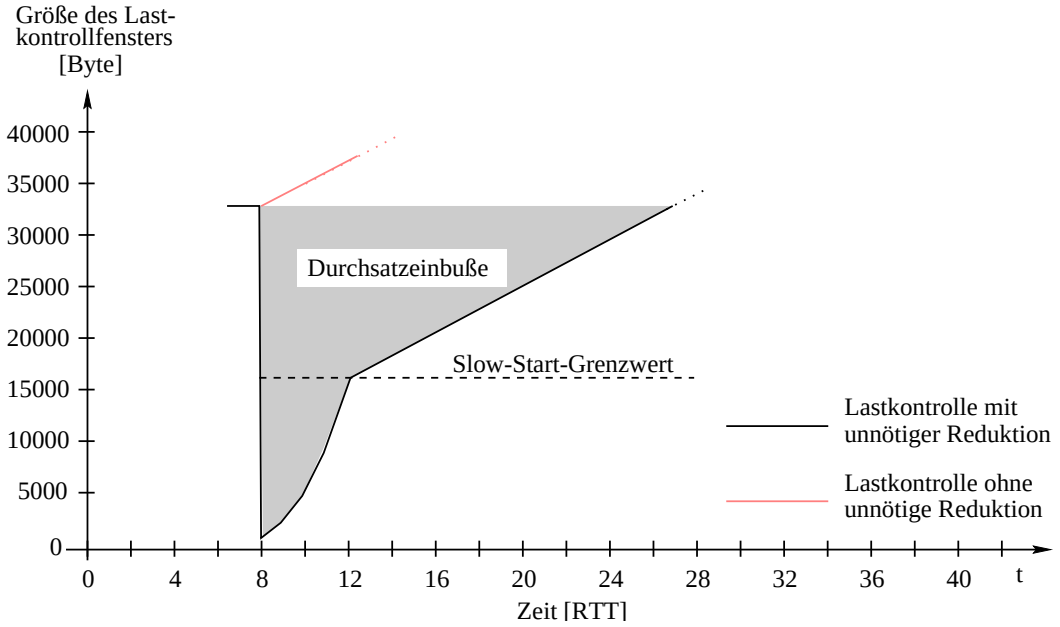


Abbildung 2.15: Durchsatzeinbußen nach einem Timeout

Es wird von 1000 Bytes großen Segmenten und von 32000 Bytes unbestätigten Nutzdaten zum Zeitpunkt des Timeouts (Zeitpunkt 8) ausgegangen. Im Zeitraum [6,8] verändert sich das Lastkontrollfenster nicht, da keine Bestätigungen empfangen werden. Erst zum Zeitpunkt 8 wird nach dem Timeout die Kommunikation wieder aufgenommen. Die durch die unnötige Lastreduktion bedingte Durchsatzeinbuße ist in Abb. 2.15 grau dargestellt. Es wird zum Zeitpunkt 8 ein Slow Start vorgenommen und ab dem Zeitpunkt 12 die Lastkontrolle durch das Congestion-Avoidance-Verfahren reguliert.

Paketverluste in mehreren aufeinanderfolgenden Paketumlaufzeiten
Werden in zwei aufeinanderfolgenden Paketumlaufzeiten Pakete nach einem Timeout wiederholt, so fallen die durch die Lastkontrolle bedingten Durchsatzeinbußen noch drastischer aus. Eine wesentliche Rolle spielt hierbei der Slow-Start-Grenzwert, der festlegt, wie lange die Öffnung des Lastkontrollfensters exponentiell erfolgt, bevor zur linearen Öffnung übergegangen wird.

Abb. 2.16 zeigt ein Szenario, in dem sowohl die erste Übertragung eines Nutzdatenpakets als auch die erste Übertragungswiederholung dieses Pakets nicht erfolgreich ist. Zum Zeitpunkt 2 erfolgt ein Timeout für das übertragene Paket. Daraufhin wird das Lastkontrollfenster auf ein Segment verkleinert, ein Slow-Start-Grenzwert von 16000 Byte verwendet und

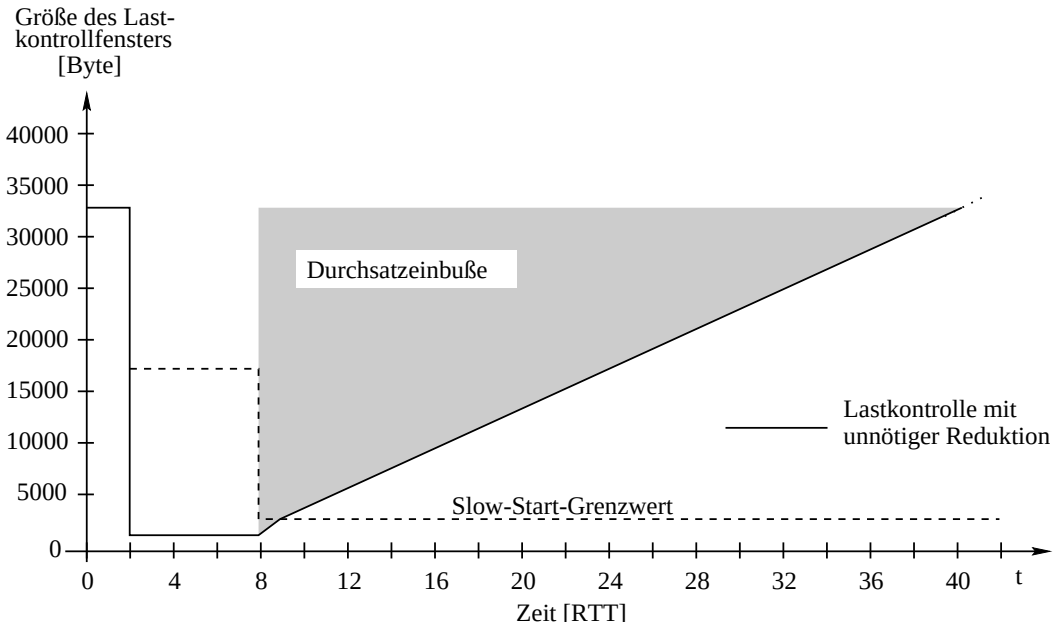


Abbildung 2.16: Durchsatzeinbußen nach aufeinanderfolgenden Timeouts

das Paket, für das der Timeout erfolgte, erneut gesendet. Der Timer wird mit dem Wert 6 RTT initialisiert. Da auch das wiederholte Paket auf Grund von Bitfehlern nicht korrekt übertragen wird, ergibt sich zum Zeitpunkt 8 erneut ein Timeout. Zwischen den beiden Timeouts zu den Zeitpunkten 2 bzw. 8 empfängt der Sender keine Bestätigungen. Somit hat das Lastkontrollfenster zum Zeitpunkt 8 weiterhin die Größe eines Segments. Als neuer Slow-Start-Grenzwert wird der Minimalwert von 2 Segmenten verwendet.

Der zweimalig fehlgeschlagene Sendeversuch eines Pakets führt wie im Beispiel gezeigt dazu, daß der Slow-Start-Grenzwert auf seinen Minimalwert gesetzt wird. Als Konsequenz entfällt bei der Adaption des Lastkontrollfensters die Phase der exponentiellen Erhöhung. Die durch die unnötige Lastreduktion bedingten Durchsatzeinbußen fallen somit noch deutlicher als in den in Abb. 2.13 und Abb. 2.15 dargestellten Szenarien aus.

2.3.2.2 Auswirkungen von Unterbrechungen

Temporäre Unterbrechungen des Übertragungskanals zwischen Sender und Empfänger stellen im Bereich der Mobilkommunikation keine Ausnahmesituation dar, sondern treten auch im regulären Betrieb auf. Basisstationswechsel, Verzögerungen, bis von Mobile IP nach einem Subnetzwechsel eines mobilen Systems das Routing angepaßt wurde, und Unterbrechungen auf dem Funkkanal können Ursache dafür sein, daß die Kommunikation zwischen dem Sender und dem Empfänger temporär unterbrochen ist. Längere Unterbrechungen können sich ergeben, falls mobile Systeme den Netzabdeckungsbereich verlassen und zu einem späteren Zeitpunkt in einen Bereich mit Funkversorgung zurückkehren. Das Transportprotokoll TCP wird mit diesen Unterbrechungen konfrontiert. Sinnvoll ist eine sofortige Wiederaufnahme der Kommunikation nach der temporären Unterbrechung und die Vermeidung unnötiger Lastreduktionen. Inwieweit TCP diese Anforderungen erfüllen kann, wird im folgenden betrachtet.

Durch Unterbrechungen bedingte Paketverluste werden von TCP ebenfalls wie auch die durch Bitfehler bedingten Paketverluste fälschlicherweise als Indiz für Überlast gewertet und

daraufhin das Lastkontrollfenster verkleinert. Die Ausführungen in Kapitel 2.3.2.1 zu dieser Problematik sind auch im Falle der durch Unterbrechungen bedingten Paketverluste zutreffend. Insbesondere die anhand Abb. 2.16 verdeutlichte Verwendung eines minimalen Slow-Start-Grenzwertes nach einer Unterbrechung ist nicht sinnvoll.

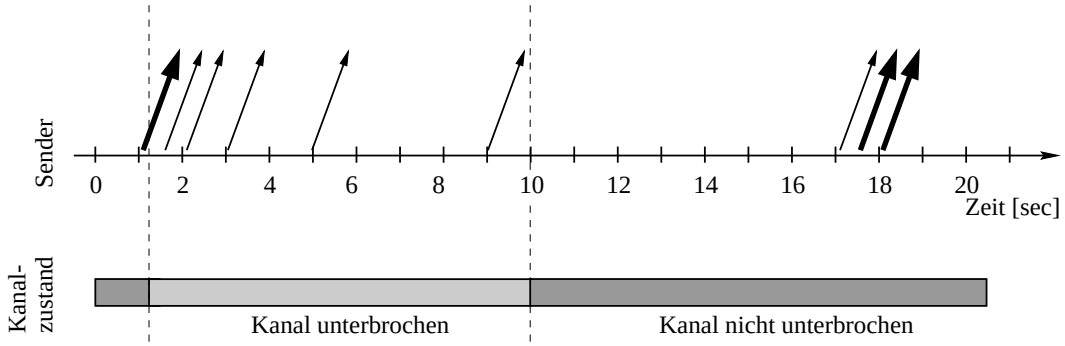


Abbildung 2.17: Verhalten von TCP bei Unterbrechungen

Hinsichtlich des Zeitpunktes, zu dem nach einer Unterbrechung die Kommunikation in der Transportschicht wieder aufgenommen wird, ist der *exponentielle Backoff*-Mechanismus von zentraler Bedeutung. Abb. 2.17 zeigt das Verhalten von TCP im Falle einer längeren Unterbrechung. Ab dem Zeitpunkt 1 sendet der Sender mehrere Nutzdatenpakete (dicker Pfeil). Da ab dem Zeitpunkt 1.25 der Funkkanal unterbrochen ist, werden nicht alle Pakete erfolgreich übertragen. Zum Zeitpunkt 1.5 erfolgt ein Timeout und das erste nicht erfolgreich übertragene Paket wird unter Kontrolle eines Timers erneut gesendet (dünner Pfeil). Der Timeoutwert beträgt 0.5 sec. Weitere Sendeversuche mit jeweils verdoppeltem Timeoutwert erfolgen zu den Zeitpunkten $2, 3, 5, 9$ und 17. Obwohl ab dem Zeitpunkt 10 der Kanal nicht mehr unterbrochen ist, werden bis zum Zeitpunkt 17 keine Nutzdatenpakete gesendet. Sinnvoll wäre eine Aufnahme der Kommunikation seitens TCP zum Zeitpunkt 10.

2.4 Zusammenfassung

Es ist davon auszugehen, daß verschiedene Mobilkommunikationssysteme in Zukunft nebeneinander existieren werden und diese Systeme durch das Internet verbunden sein werden. Um die Mobilität eines Endsystems auch zwischen verschiedenen Mobilkommunikationssystemen zu unterstützen, ist eine Mobilitätsunterstützung erforderlich. Für IPv4 bietet das Mobile IP Protokoll diese Unterstützung.

Es ist allerdings nicht ausreichend, für mobile Systeme lediglich die Anbindung auf IP-Ebene, z.B. mittels Mobile IP, zu realisieren. Es muß zusätzlich betrachtet werden, inwieweit die Übertragungseigenschaften der drahtlosen Übertragung sich auf die Performance auswirken. Höhere Fehlerraten und durch Basisstationswechsel, Subnetzwechsel oder temporäres Verlassen des Funkabdeckungbereiches bedingte Unterbrechungen sind typisch für die drahtlose Kommunikation. Unter diesen Übertragungsbedingungen erweist sich der Einsatz von TCP als problematisch, da das Lastkontrollfenster und der Slow-Start-Grenzwert unnötigerweise verkleinert werden. Darüber hinaus nimmt TCP nicht unmittelbar am Ende einer Unterbrechung des Übertragungskanals die Kommunikation wieder auf. In der Literatur beschriebene Lösungsansätze für die genannten Probleme werden in Kapitel 3 ausführlich diskutiert.

Kapitel 3

Stand der Forschung

Längere Unterbrechungen des Übertragungskanals und durch Übertragungsfehler auf dem drahtlosen Link bedingte Paketverluste, die fälschlicherweise TCP zur Reduktion der Last veranlassen, sind, wie im vorangegangenen Kapitel ausgeführt, die Hauptursache für die Performance Probleme von TCP in drahtlosen Umgebungen. In der Literatur sind für diese Probleme eine Vielzahl verschiedener Ansätze beschrieben. Sie adressieren häufig nur einen Teil der im Umfeld der drahtlosen Kommunikation auftretenden Probleme und unterscheiden sich dahingehend, in welcher Schicht des Protokollstacks die für die Problemlösung vorgeschlagenen Mechanismen angesiedelt sind.

Um eine Einordnung der in der Literatur beschriebenen Lösungsvorschläge zu erleichtern, werden in Kapitel 3.1 zunächst Klassifikationskriterien vorgestellt. Bei der Beschreibung der einzelnen Lösungsansätze wird auf diese Kriterien eingegangen. Hinsichtlich der Klassifikation eines Verfahrens, das die durch die drahtlose Übertragung bedingten Probleme adressiert, ist es ein wesentliches Kriterium, ob das Verfahren Ende-zu-Ende oder in der lokalen Umgebung des drahtlosen Links operiert. Ende-zu-Ende-Verfahren sind in Kapitel 3.2 beschrieben, lokale Verfahren in Kapitel 3.3. Der indirekte Transportansatz kristallisiert sich in der in Kapitel 3.4 beschriebenen Bewertung der verschiedenen Ansätze als der am besten geeignete Ansatz für die gestellten Anforderungen heraus. In Kapitel 3.5 werden im Kontext indirekter Transportansätze auftretende Probleme analysiert. Ein zentrales Problem ist, daß indirekte Transportansätze auf Grund der zusätzlich im Netz zu verwaltenden Statusinformation eine spezielle – über die globale Mobilitätsunterstützung hinausgehende – Mobilitätsunterstützung benötigen. Sie wird als *Mobilitätsunterstützung für indirekte Transportansätze* bezeichnet. Die *Migration mit Einfrieren*, ein mögliches Verfahren für die Mobilitätsunterstützung indirekter Transportansätze, wird in Kapitel 3.5 vorgestellt.

3.1 Klassifikation von Lösungsansätzen

Eine Einordnung der Lösungsansätze kann anhand der jeweils adressierten Probleme vorgenommen werden. Darüber hinaus existieren konzeptionelle Unterschiede, die ebenfalls eine Basis für eine Klassifikation bilden können. Auf beide Gruppen von Klassifikationskriterien wird im folgenden eingegangen.

3.1.1 Adressierte Probleme

Um eine Internetanbindung auch für drahtlos angebundene, mobile Systeme zu realisieren, müssen folgende Aspekte von den für die Problemlösung vorgeschlagenen Ansätzen berücksichtigt werden:

- Höhere Bitfehlerraten
  Wie in Kapitel 2.1.4 dargelegt, kann nicht davon ausgegangen werden, daß sich die Bitfehlerraten in drahtlosen Netzen in einer ähnlichen Größenordnung wie im Bereich der Festnetze bewegen. Aus diesem Grunde sind Mechanismen notwendig, die höhere Bitfehlerraten adressieren.

- Häufigere Unterbrechungen des Übertragungskanals
  Unterbrechungen des Übertragungskanals sind, wie in Kapitel 2.1.4 skizziert, eine typische Situation, mit der im drahtlosen Umfeld gerechnet werden muß. Geeignete Mechanismen sind erforderlich, um eine schnelle Wiederaufnahme der Datenkommunikation in der Transportschicht nach dem Ende der Unterbrechung des Funkkanals zu ermöglichen. Darüber hinaus muß vermieden werden, daß der Slow-Start-Grenzwert von TCP während der Unterbrechung auf seinen Minimalwert verringert wird.

- Mobilität der Endsysteme
  Einige Ansätze gehen von drahtlos angeschlossenen, aber stationären Endsystemen aus. Sie adressieren zwar höhere Bitfehlerraten und häufigere Unterbrechungen, sind aber auf Grund der verwendeten Mechanismen nur einsetzbar, falls das Endsystem nicht mobil ist. Ursache ist eine fehlende Mobilitätsunterstützung. Andere Ansätze schlagen hingegen Mechanismen zur Kompensation des fehleranfälligen Links vor, die auch im Falle der Mobilität der Endsysteme noch einsetzbar sind.

3.1.2 Konzeptionelle Unterschiede der Lösungsansätze

Die Lösungsansätze lassen sich nicht nur anhand der Probleme klassifizieren, die sie zu lösen versuchen, sondern auch anhand der den Lösungen zugrundeliegenden Konzepte. Auch wesentliche Unterschiede der einzelnen Lösungen können als Unterscheidungskriterien dienen. Auf folgende Kriterien wird bei der Beschreibung der verschiedenen Lösungsansätze eingegangen:

- Ende-zu-Ende-Lösungen vs. lokale Lösungen
  Bei *Ende-zu-Ende-Lösungen* wird in den Endsystemen das TCP-Protokoll modifiziert. Es existieren sowohl Lösungen, die eine schnellere Übertragungswiederholung veranlassen, als auch solche, die unnötige Lastreduktionen von TCP im Umfeld der funkbasierten Übertragung zu vermeiden versuchen. Alternativ kann auch mittels *lokaler Lösungen* versucht werden, die Fehleranfälligkeit drahtloser Übertragungsstrecken in der lokalen Umgebung dieser Strecken durch geeignete Korrekturverfahren zu kompensieren. Die TCP-Instanzen werden dann nicht mit den höheren Bitfehlerraten dieser Strecken konfrontiert. Unnötige Lastreduktionen auf Grund von Übertragungsfehlern treten somit seltener auf.

- Modifizierte Protokollschicht
  Ein weiteres Unterscheidungsmerkmal der Lösungen besteht darin, in welcher Protokollschicht der vorgeschlagene Mechanismus realisiert wird.

- Modifikationen an den Festnetzrechnern
  Hinsichtlich der notwendigen Modifikationen stellen die verschiedenen Ansätze verschieden starke Anforderungen. Bei manchen Ansätzen sind die Modifikationen auf das mobile Endsystem beschränkt, andere erfordern sogar Änderungen an den Kommunikationspartnern im Festnetz.

- TCP Ende-zu-Ende-Semantik
  Ein weiteres Unterscheidungskriterium ist, inwieweit die TCP *Ende-zu-Ende-Semantik* durch einen Lösungsansatz verändert wird. TCP-Bestätigungspakete informieren normalerweise den Sender darüber, daß ein entsprechendes Paket erfolgreich zur Transportinstanz des empfangenden Endsystems übertragen wurde. Bei Lösungsansätzen, die die Ende-zu-Ende-Semantik ändern, kann hingegen aus dem Empfang eines Bestätigungspakets nicht geschlossen werden, daß das bestätigte Nutzdatenpaket erfolgreich bei der Transportinstanz des empfangenden Endsystemes ausgeliefert wurde.

- Zusätzliche netzinterne Statusinformation
  Darüber hinaus unterscheiden sich die Lösungsansätze dahingehend, inwieweit sie die Verwaltung zusätzlicher Statusinformation innerhalb des Netzes erfordern. Einige Ansätze sind zwingend auf diese Statusinformation angewiesen, andere können zwar prinzipiell auch ohne diese Statusinformation operieren, können dann aber nicht den Zweck erfüllen, trotz fehleranfälliger drahtloser Teilstrecken eine performante Datenübertragung zu ermöglichen.

- Migrationsunterstützung erforderlich bzw. realisiert
  Erfordert ein Lösungsansatz Statusinformation innerhalb des Netzes, so muß diese im Falle eines Ortswechsels eines mobilen Systems ggf. auf einem anderen Zwischensystem verfügbar gemacht werden. Dies ist die Aufgabe der *Migrationsunterstützung*. Die Lösungsansätze unterscheiden sich dahingehend, inwieweit eine Migrationunterstützung notwendig ist und in dem jeweiligen Lösungsansatz mit betrachtet wird.

Die in der Literatur beschriebenen Ansätze lassen sich in zwei große Klassen einteilen: Ende-zu-Ende-Lösungsansätze und in der lokalen Umgebung der drahtlosen Teilstrecke operierende Ansätze. Ende-zu-Ende-Lösungen, bei denen in der Schicht 4, d.h. an den TCP-Instanzen der Endsysteme Modifikationen vorgenommen werden, werden in Kapitel 3.2 beschrieben. Lokale Lösungen werden in Kapitel 3.3 behandelt und können in drei Unterklassen eingeteilt werden: Lösungen in der Schicht 2, Lösungen in der Schicht 3 und Lösungen in der Schicht 4. Ohne auf die einzelnen Lösungsansätze innerhalb einer Klasse bzw. Unterklasse einzugehen, wird für jede der Klassen bzw. Unterklassen betrachtet und tabellarisch zusammengefaßt, inwieweit Modifikationen an den Festnetzrechnern erforderlich sind, die TCP Ende-zu-Ende-Semantik verändert wird und zusätzlich netzinterne Statusinformation notwendig ist. Darüber hinaus ist in die Tabellen mit aufgenommen, inwieweit eine Migrationsunterstützung erforderlich und realisiert ist. Bei der Beschreibung der einzelnen Lösungsansätze wird darauf eingegangen, ob sie höhere Bitfehlerraten oder häufige Unterbrechungen des Übertragungskanals adressieren.

3.2 Ende-zu-Ende-Lösungen

Abb. 3.1 zeigt das grundlegende Szenario der Ende-zu-Ende-Lösungen. Modifikationen sind – in der Abbildung dunkelgrau dargestellt – am TCP-Protokoll im Festnetzrechner bzw. mobilen System erforderlich. Ansätze, die für TCP eine Lastkontrolle auf Basis expliziter Feedbacksignale vorschlagen, erfordern darüber hinaus Änderungen an den Zwischensystemen, um diese Signale zu generieren. Diese Änderungen sind in Abb. 3.1 hellgrau dargestellt.

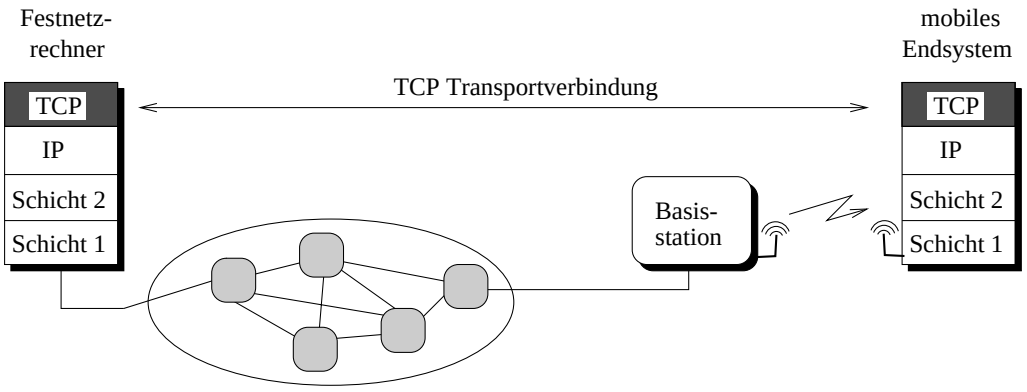


Abbildung 3.1: Ende-zu-Ende-Lösung

Bei Ende-zu-Ende-Lösungsansätzen muß die TCP-Implementierung des Festnetzrechners modifiziert werden. Die Ende-zu-Ende-Semantik von TCP bleibt erhalten. Netzinterne Statusinformation muß weder verwaltet noch migriert werden (siehe Tabelle 3.1).

Modifikation der Festnetzrechner	TCP Ende-zu-Ende-Semantik	zusätzliche Statusinformation	Migrationssupport für Statusinformation
notwendig	unverändert	nicht notwendig	nicht notwendig
realisiert			nicht realisiert

Tabelle 3.1: Klassifikation der betrachteten Ende-zu-Ende-Lösungen

3.2.1 Optimierung der Fehlerkorrektur

Um die Fehlerkorrektur von TCP zu optimieren, bieten sich mehrere Ansatzpunkte an. Es kann die Strategie, die die zu wiederholenden Pakete bestimmt, optimiert werden. Darüber hinaus können auch an dem timerbasierten Mechanismus, der für das Veranlassen einer Übertragungswiederholung verantwortlich ist, Verbesserungen vorgenommen werden.

3.2.1.1 Modifikation der Bestätigungs- und Wiederholungsstrategie

[MMFR96] beschreibt sogenannte *selektive Bestätigungen* für TCP (TCP-Sack). Im Gegensatz zur kumulativen Bestätigung können einzelne Pakete bestätigt werden. Insbesondere kann auch dann bestätigt werden, wenn Nutzdaten mit niedrigerer Sequenznummer noch nicht erfolgreich empfangen wurden. Die selektiv bestätigten Sequenznummern werden im TCP-Optionen-Feld kodiert. Für die Protokollverarbeitung sind sowohl im Sender als auch im

Empfänger Änderungen an der TCP-Implementierung erforderlich. Selektive Bestätigungen ermöglichen es – im Gegensatz zum Fast-Retransmit-Mechanismus – auch im Falle mehrerer Paketverluste pro Paketumlaufzeit diese zügig zu korrigieren und unter Umständen einen Timeout mit anschließender Slow-Start-Phase zu vermeiden. In [BHZ98] wird der positive Einfluß selektiver Bestätigungen und selektiver Übertragungswiederholungen auf die Geschwindigkeit und die Effizienz der Fehlerkorrektur von TCP nachgewiesen. In [SF98] beschreiben die Autoren, daß insbesondere im drahtlosen Umfeld mit fehleranfälligen Übertragungskanälen die Verwendung selektiver Bestätigungen sinnvoll ist. Darüber hinaus schlagen sie ein Verfahren vor, das es erlaubt, den Verlust von wiederholten Nutzdatenpaketen zu erkennen und diese erneut zu übertragen, ohne auf den zugehörigen Timeout warten zu müssen. Das Verfahren analysiert die eingehenden Bestätigungen und entscheidet daraufhin, welche Nutzdatenpakete wiederholt werden müssen.

Die in RFC 2018 [MMFR96] spezifizierten selektiven Bestätigungen erhalten inzwischen zunehmend Einzug in die Betriebssysteme. Selektive Bestätigungen sind in Windows 98, Windows 2000, Linux (ab der Version 2.2) und Solaris (ab der Version 2.7) implementiert. In [All00] beschriebene Messungen ergaben, daß der Anteil der TCP-Verbindungen, die beim Verbindungsaufbau TCP-Sack anfordern, im Zeitraum Dezember 1998 bis Februar 2000 von ca. 5% auf ca. 20% angestiegen ist. Von einem weiteren Anstieg des Anteils der TCP-Verbindungen, die TCP-Sack anfordern, ist auszugehen.

3.2.1.2 Optimierung der timerbasierten Übertragungswiederholung

Hauptproblem der timerbasierten Übertragungswiederholung ist es, daß zum Sendezeitpunkt eines Pakets die Zeitdauer bis zum Empfang des zugehörigen Bestätigungspakets nicht bekannt ist und somit die Wahl eines geeigneten Timeoutwertes schwer ist. TCP bestimmt aus Messungen der Paketumlaufzeiten den zu verwendenden Timeoutwert. Verbesserungen lassen sich erzielen, indem exaktere Schätzmethoden Grundlage für die Bestimmung des Timeoutwertes werden.

Exaktere und häufigere Messung der Paketumlaufzeit
Der standardmäßig in TCP implementierte Karn-Algorithmus [KP87] legt fest, daß für wiederholte Pakete keine Paketumlaufzeiten zu messen sind und kein neuer Timeoutwert zu berechnen ist. Mittels der in Kapitel 2.3.1.1 beschriebenen Zeitstempel-Option (TCP-Zeitstempel) lassen sich dagegen häufigere und exaktere Messungen der Paketumlaufzeit realisieren [Ste94], [JBB92], da auch für wiederholte Pakete eine Messung vorgenommen werden kann. Gerade im Umfeld der drahtlosen Kommunikation mit häufigen und starken Schwankungen der Paketumlaufzeit und häufigen Übertragungswiederholungen sind exaktere Messungen von Vorteil. Häufigere Messungen der Paketumlaufzeit sind insbesondere dann nützlich, wenn nach mehrmaligen aufeinanderfolgenden Timeouts auf Grund des exponentiellen Backoff-Mechanismus pessimistische und große Timeoutwerte zum Einsatz kommen. Die Verwendung der Zeitstempel-Option ermöglicht es in diesem Fall frühzeitiger, einen optimistischeren und realistischeren Timeoutwert anstatt des pessimistischen, durch mehrmalige exponentielle Anpassung vergrößerten Timeoutwertes zu verwenden. Wird in diesem Szenario eine Übertragungswiederholung nach einem Timeout erforderlich, so kann diese auf Grund des realistischer gewählten Timeoutwertes schneller veranlaßt werden. Die Verwendung von Zeitstempeln wird in [Lud00],

[PGLA99] als ein Mechanismus angeführt, der zusätzlich zu den jeweils dort beschriebenen Mechanismen gewinnbringend eingesetzt werden kann. Allerdings ist der Algorithmus, der dann in TCP aus den gemessenen Paketumlaufzeiten den neuen Timeoutwert bestimmt [JK98], nur bedingt geeignet, falls häufige RTT-Messungen mit feingranularer Auflösung im Bereich von 10 ms vorgenommen werden. Dies wird in [LS00] diskutiert und es wird zusätzlich eine neue Variante der Timeoutberechnung vorgeschlagen.

Vermeidung unnötiger Timeouts
Sogenannte *Auxiliary Timeouts* werden in [CL97] beschrieben, um TCP resistenter gegenüber stärkeren Schwankungen der Paketumlaufzeit zu machen. Es wird vorgeschlagen, nicht unmittelbar nach einem Timeout eine Übertragungswiederholung und eine Reduktion der Last zu veranlassen, sondern noch eine zusätzliche Zeitdauer abzuwarten, ob das jeweilige Bestätigungspaket nicht doch noch beim Sender eintrifft. Ist dies der Fall, so erfolgen keine Übertragungswiederholungen und keine Lastreduktion. Andernfalls werden, wie in TCP spezifiziert, Nutzdatenpakete wiederholt und die Last reduziert. Die zusätzlich zu wartende Zeitdauer wird auf Basis der Verspätungen, die für in der Vergangenheit verspätet eingetroffene Bestätigungen gemessen wurden, bestimmt. Nachteil dieses Verfahrens ist, daß im Fall einer notwendigen Übertragungswiederholung diese zusätzlich verzögert wird.

Optimierungen im Fall von Unterbrechungen
Nach Unterbrechungen des Übertragungskanals wird erst nach Ablauf des während der Unterbrechung exponentiell vergrößerten Timers die Übertragungswiederholung veranlaßt. Es vergeht somit ggf. zwischen dem Ende der Unterbrechung und der Wiederaufnahme der Kommunikation auf der Transportebene eine signifikante Zeitdauer (siehe Kapitel 2.3.2.2). Um eine schnelle Aufnahme der Kommunikation zu veranlassen, wird in [CI95] vorgeschlagen, vom mobilen System drei Bestätigungsduplikate zum Kommunikationspartner zu senden und diesen somit zu veranlassen, mittels Fast Retransmit die Kommunikation fortzusetzen. Das Verfahren wird als *künstliches Fast Retransmit* bezeichnet. Es ermöglicht zwar eine schnelle Wiederaufnahme der Kommunikation, den negativen Auswirkungen des auf Grund des Timeouts auf den Minimalwert gesetzten Lastkontrollfensters und Slow-Start-Grenzwertes kann es aber nicht entgegenwirken.

[GMPG00] adressiert ebenfalls die sich durch eine Unterbrechung des Übertragungskanals für die timerbasierte Übertragungswiederholung ergebenden Probleme. Es wird davon ausgegangen, daß die TCP-Instanz des mobilen Systems vor der Unterbrechung noch über die bevorstehende Unterbrechung informiert werden kann und die TCP-Instanz noch ein TCP-Paket zum Kommunikationspartner senden kann. In diesem Paket ist der Sendekredit auf 0 gesetzt. Der Kommunikationspartner wechselt daraufhin in den Persist-Modus, d.h. der die Übertragungswiederholungen veranlassende Timer wird eingefroren. Übertragungswiederholungen und Reduktionen des Lastkontrollfensters und des Slow-Start-Grenzwertes werden deshalb während der Unterbrechung nicht vorgenommen.

3.2.2 Verbesserung der Lastkontrolle

Die im folgenden beschriebenen Ansätze verfolgen das Ziel, die Lastkontrolle von TCP dahingehend zu modifizieren, daß durch eine fehlerhafte Übertragung über dem drahtlosen Link be-

dingte Paketverluste nicht fälschlicherweise eine Lastreduktion bewirken. Grundsätzlich kann hierbei zwischen Verfahren unterschieden werden, die wie TCP auf impliziten Signalen beruhen, und Verfahren, die explizite Feedback-Signale nutzen. Als Ende-zu-Ende operierende Verfahren sind die Verfahren zur Verbesserung der Lastkontrolle wie in Tabelle 3.1 dargestellt einzuordnen.

Explizite Feedbacksignale
[Flo94], [GCW98], [BKVP97], [CRVP98] schlagen Verfahren vor, wie explizite Signale dazu eingesetzt werden können, auch im Umfeld der Mobilkommunikation mit den dort typischen Übertragungseigenschaften unnötige Lastreduktionen zu vermeiden. Zwei verschiedene Typen von expliziten Feedbacksignalen werden in der Literatur vorgeschlagen: Explizite Überlastsignale, explizite Paketverlustsignale.

Explizite Überlastsignale werden in [GCW98], [Flo94] und [RF99] eingesetzt, um im Falle einer Überlast im Zwischensystem den Sender über diese Überlastsituation zu informieren. Weiterhin wird der Sender dahingehend modifiziert, daß nicht mehr Paketverluste als Indiz für Überlast herangezogen werden, sondern ausschließlich bei Empfang expliziter Überlastsignale die Last reduziert wird. Durch Übertragungsfehler auf dem drahtlosen Link bedingte Paketverluste haben somit nicht mehr eine Reduktion der Last seitens des Senders zur Folge.

Explizite Paketverlustsignale werden in [BKVP97] und [CRVP98] diskutiert, um unnötige Lastreduktionen zu vermeiden. Paketverluste werden allerdings weiterhin – wie auch in TCP spezifiziert – als Indiz für eine Überlastsituation herangezogen. Zusätzlich wird der Sender aber mittels expliziter Signale über Situationen, die Paketverluste zur Folge haben, aber keine Lastreduktion erfordern, informiert. Empfängt der Sender derartige Signale, so verzichtet er trotz eines Paketverlustes auf eine Lastreduktion. In [BKVP97] werden von der Basisstation generierte explizite Feedbacksignale beschrieben, um den Sender über Zeiträume schlechter Übertragungseigenschaften – und damit erhöhter Paketverlustraten – auf dem Funkkanal zu informieren. In Multi-Hop-Netzwerken, bei denen Pakete über andere mobile Systeme zum Zielsystem geroutet werden, treten häufiger Situationen auf, in denen mobile Systeme nicht erreichbar sind. [CRVP98] schlägt in diesem Fall vor, den Sender über eine derartige Situation zu informieren und Paketverluste dann nicht als Indiz für Überlast zu werten.

Implizite Feedbacksignale
Untersuchungen, inwieweit implizite Feedbacksignale dazu geeignet sind, unnötige Lastreduktionen zu vermeiden, die durch Paketverluste bei der Übertragung über drahtlosen Links bedingt sind, sind in [BV98] und [LK00] zu finden.

Im Endsystem gemessene Paketumlaufzeiten als implizites Signal heranzuziehen, um zwischen durch Überlast bzw. durch Übertragungsfehler bedingten Paketverlusten zu unterscheiden, wird in [BV98] untersucht. Die betrachteten Verfahren eignen sich allerdings nicht, um die Ursache eines Paketverlustes zu ermitteln. Sie können somit nicht als Kriterium für die Entscheidung dienen, ob eine Überlast vorliegt und die Last reduziert werden muß.

TCP-Eifel [LK00] verwendet ebenfalls implizite Signale. Anhand des impliziten Signals kann zum Zeitpunkt des Timeouts allerdings nicht entschieden werden, ob eine Überlast vorliegt. Stattdessen kommt ein implizites Signal zum Einsatz, dem zu einem späteren Zeitpunkt, d.h. nach dem Timeout, entnommen werden kann, daß ggf. keine Überlast vorgelag. Es wird zum Zeitpunkt des Timeouts also nicht versucht zu entscheiden, ob eine Überlast vorliegt

und eine Lastreduktion erforderlich ist. Stattdessen wird im Falle eines Timeouts generell die Last reduziert. Empfängt der Sender zu einem späteren Zeitpunkt eine Bestätigung für das Nutzdatenpaket, für das der Timeout erfolgt ist, so wird die Lastreduktion wieder rückgängig gemacht, d.h. das Lastkontrollfenster auf seine ursprüngliche Größe gesetzt. Ursache für diese Verspätung können beispielsweise mehrmalige Übertragungswiederholungen in der Schicht 2 sein. Der Empfang des jeweiligen Bestätigungspakets wird also als implizites Signal dafür gewertet, daß keine Überlast vorgelag. Das beschriebene Verfahren kann dazu eingesetzt werden, unnötige Lastreduktionen, die durch den verspäteten Empfang von Bestätigungspaketen bedingt sind, rückgängig zu machen [Lud00].

3.3 Lokale Lösungen

Mittels der lokalen Lösungen wird versucht, die durch die Fehleranfälligkeit des drahtlosen Links bedingten Übertragungsfehler durch geeignete Maßnahmen in der lokalen Umgebung des drahtlosen Links zu vermeiden oder zu korrigieren. Ziel dieser Maßnahmen ist es, die Zahl der für TCP feststellbaren Paketverluste auf eine ähnliche Größenordnung wie bei der drahtgebundenen Übertragung zu reduzieren. Gelingt dies, so ist der in TCP verfolgte Ansatz, Paketverluste als Indiz für Überlast zu werten, auch dann vertretbar, wenn der Pfad zwischen Sender und Empfänger einen fehleranfälligen drahtlosen Link beinhaltet. Die lokal angesiedelten Mechanismen können allerdings nicht für sich alleine betrachtet werden, da sie unter Umständen Auswirkungen auf höhere Schichten des Protokollstacks haben. Insbesondere sich ggf. ergebende zusätzliche Verzögerungen können trotz erfolgreicher Übertragung auf Grund dann verspätet eintreffender Bestätigungspakete einen Timeout in der TCP-Instanz des Senders zur Folge haben. In diesem Fall wird trotz der erfolgreichen Übertragung des Pakets die Last reduziert.

Die verschiedenen in der Literatur beschriebenen Ansätze lassen sich danach einordnen, in welcher Schicht des Protokollstacks sie angesiedelt sind. Sie werden in den folgenden Unterkapiteln detaillierter beschrieben.

3.3.1 Lösungsansätze in der Schicht 1 bzw. Schicht 2

Abb. 3.2 zeigt das grundlegende Szenario für auf Schicht 1 bzw. Schicht 2 operierende Lösungsansätze. Die für die Realisierung dieser Ansätze notwendigen Änderungen sind lokaler Natur, d.h. auf die für den Zugriff auf den Funkkanal verantwortlichen Komponenten der Basisstation und des mobilen Systems beschränkt.

Modifikationen an der TCP-Implementierung werden weder beim Festnetzrechner noch beim mobilen System vorgenommen. Darüber hinaus bleibt die Ende-zu-Ende-Semantik erhalten. Ein Teil der Ansätze kommt ohne zusätzliche Statusinformation aus, andere benötigen diese. Die Statusinformation, die für die Übertragungswiederholung zwischengespeicherte Pakete umfaßt, wird allerdings im Fall eines Basisstationswechsels nicht zur neuen Basisstation übertragen. Deshalb sind unmittelbar nach einem Basisstationswechsel keine lokalen Wiederholungen möglich. Tabelle 3.2 faßt die Merkmale der in der Schicht 2 angesiedelten lokalen Mechanismen zusammen.

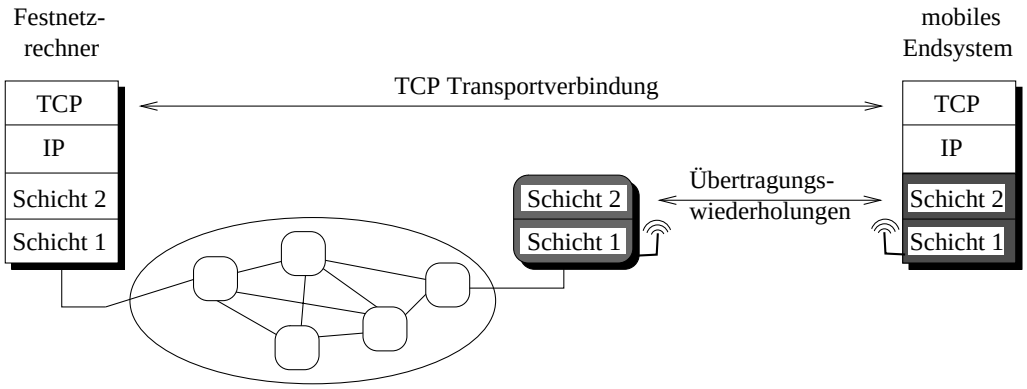


Abbildung 3.2: Schicht 1 und Schicht 2 Lösungen

Modifikation der Festnetzrechner	TCP Ende-zu-Ende-Semantik	zusätzliche Statusinformation	Migrationssupport für Statusinformation
nicht notwendig	unverändert	teilweise notwendig	bedingt notwendig
nicht realisiert			nicht realisiert

Tabelle 3.2: Klassifikation der betrachteten lokalen Lösungen (Schicht 2)

Wesentlicher Vorteil der auf Schicht 1 bzw. Schicht 2 operierenden Ansätze ist, daß bei der Entscheidung, mit welchen Mitteln die Fehleranfälligkeit des drahtlosen Links kompensiert wird, die aktuellen Übertragungseigenschaften des drahtlosen Links mit berücksichtigt werden können. Auf schnell wechselnde und stark schwankende Übertragungseigenschaften der Funkkanals kann bei diesen Ansätzen gezielt reagiert werden. Mögliche Reaktionen sind:

- Wahl des Sendezeitpunktes,
- Veränderung der Kodierung und der Menge hinzugefügter Redundanz,
- Segmentierung und gezielte Wahl der zu sendenden Paketlängen und
- Übertragungswiederholungen in der Schicht 2.

In [BBKT97] wird vorgeschlagen, Pakete nicht sofort auf den Funkkanal zu senden, sondern stattdessen die aktuellen Übertragungseigenschaften mit zu berücksichtigen und erst dann zu senden, wenn die Übertragungseigenschaften akzeptabel sind. In der Literatur wird dieser Ansatz als 'channel state dependent scheduling' bezeichnet. Anstatt zu warten, bis sich akzeptable Übertragungseigenschaften auf dem Funkkanal ergeben, können auch aktiv Maßnahmen ergriffen werden, um eine weniger fehleranfällige Übertragung zu ermöglichen. Dies läßt sich durch die Verwendung eines anderen Kodierungsverfahrens oder durch Hinzufügen von zur Fehlerkorrektur nutzbarer Redundanz erreichen. Adaptive Verfahren [ES98b] lassen sich hierzu gewinnbringend einsetzen. In [ZR97] wird beschrieben, die adaptiven Verfahren nach Möglichkeit so zu konzipieren, daß zwar die Zahl der Fehler reduziert wird, Fehler aber weiterhin in Bursts auftreten. Dies erfolgt vor dem Hintergrund, daß TCP – in der Variante ohne selektive Bestätigungen – mit Sequenzen fehlender Pakete besser zurechtkommt, als mit gleichmäßig verteilten einzelnen Paketverlusten. Als weitere adaptive Maßnahme kann die Länge der auf dem Funkkanal übertragenen Pakete an die aktuellen Übertragungseigenschaften des Funkkanals angepaßt werden [ES98b], [BKVP97], [LS98].

Übertragungswiederholungen auf der Schicht 2 werden in einer Vielzahl von Veröffentlichungen – teilweise zusätzlich zu weiteren Mechanismen – vorgeschlagen [BKVP97], [ES98b], [EALSG95], [LKJK99], [PGLA00], [FRSW98], [WT98]. Auch in kommerziell erhältlichen Produkten kommen Übertragungswiederholungen in der Schicht 2 zum Einsatz. ARLAN [ARL97], IEEE 802.11 [IEE99], WaveLAN 802.11 [Wav99] und der nicht transparente Übertragungsmodus von GSM [EV97] nutzen diese Technik. Bei Systemen, die Übertragungswiederholungen in der Schicht 2 unterstützen, muß zwischen solchen unterschieden werden, die für Pakete aller Datenströme ggf. Paketwiederholungen veranlassen und solchen, die nur Pakete eines zuverlässigen Protokolls ggf. wiederholen. In [Lud99] und [PGLA00] wird vorgeschlagen, für Pakete von TCP-Strömen ggf. Schicht 2 Wiederholungen vorzunehmen, für UDP-Ströme hingegen nicht.

Durch Übertragungswiederholungen bedingte Probleme
Übertragungswiederholungen in der Schicht 2 verlängern die Paketumlaufzeit von TCP-Paketen. Unter Umständen ist senderseitig ein Timeout mit anschließender Paketwiederholung und Lastreduktion die Folge, obwohl das zugehörige TCP-Paket nach mehrmaliger Wiederholung in der Schicht 2 erfolgreich übertragen werden konnte. Es muß also das Ziel sein, möglichst schnell Übertragungsfehler auf der Schicht 2 zu korrigieren. Während bei [EALSG95] erst frühstens nach der Übertragung eines kompletten Flußkontrollfensters der Schicht 2 ein Paket wiederholt werden kann, erfolgen in [PGLA00] Schicht 2 Wiederholungen selektiv und werden auf Grund sofortiger Information des Senders bzgl. einer fehlgeschlagenen Übertragung schneller veranlaßt. Um zu vermeiden, daß Paketwiederholungen die Übertragung nachfolgender Pakete verzögern, wird in [FRSW98] für CDMA Systeme vorgeschlagen, für die Wiederholungen einen anderen, d.h. weiteren Code zu verwenden und das zu wiederholende Paket zeitlich parallel zum nachfolgenden Paket zu senden.

Das Phänomen konkurrierender Übertragungswiederholungen in TCP und in der Schicht 2 ist in der Literatur beschrieben. Allerdings herrscht keine Einigkeit, ob dies tatsächlich ein Problem ist oder nicht. In [DCY93], [KRL+97], [RSW98] wird es als Problem dargestellt, während in [LRK+99] festgestellt wird, daß TCP sich den stärkeren Schwankungen der Paketumlaufzeit anpassen kann. Ursache für diese konträren Ergebnisse sind die verschiedenen verwendeten TCP-Implementierungen. Während die TCP-Implementierung von Linux Timer mit einem Minimalwert von 200 ms und einer Granularität von 10 ms verwendet, ist der Minimalwert von BSD-basierten TCP-Implementierungen 500 ms und beträgt die Granularität 500 ms. Durch Schicht 2 Wiederholungen bedingte längere Ende-zu-Ende-Paketumlaufzeiten führen im Falle von Timern mit geringerem Minimalwert und geringerer Granularität dann häufiger zu unnötigen Timeouts als bei tendenziell groß gewählten Timeoutwerten. Vor diesem Hintergrund wird klar, warum bei der Vermessung eines Linux Protokollstacks [RSW98] konkurrierende Übertragungswiederholungen der Schicht 2 und Schicht 4 beobachtet werden, wohingegen dies bei der Vermessung des BSD-basierten Protokollstacks [LRK+99] nicht der Fall ist.

Der TCP-Eifel Ansatz von Ludwig et. al. [LK00] zeichnet sich dadurch aus, daß nicht nur Übertragungswiederholungen auf der Schicht 2 vorgeschlagen werden, sondern zugleich auch Mechanismen beschrieben werden, wie auf die Lastreduktion von TCP wegen verlängerter Paketumlaufzeiten reagiert werden kann. Da es sich hierbei um ein Ende-zu-Ende operierendes Verfahren handelt, ist es bereits in Kapitel 3.2.2 beschrieben.

3.3.2 Lösungsansätze in der Schicht 3

In Abb. 3.3 ist das grundlegende Szenario dargestellt. Protokollinstanzen, die für die Umsetzung dieser Ansätze modifiziert werden müssen, sind grau unterlegt dargestellt. Veränderungen an den Schichten 1 und 2 der Basisstation bzw. des mobilen Systems sind nicht erforderlich.

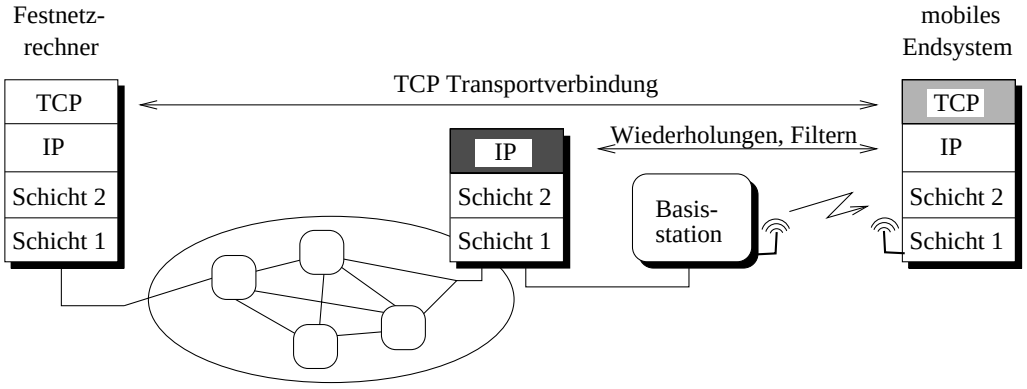


Abbildung 3.3: Schicht 3 Lösungen

Kernidee der in der Schicht 3 angesiedelten Lösungsansätze ist es, im Router vor dem drahtlosen Link die Protokollköpfe der TCP-Pakete auszuwerten und auf Basis dieser Information zu bestimmen, welche Pakete über den drahtlosen Link gesendet werden. Diese Auswertung erfolgt in der Netzwerkschicht des Routers. Hierzu werden in dem Router die Sequenznummern bzw. die Bestätigungssequenznummern der passierenden TCP-Pakete analysiert. Das Schichtenprinzip wird hierbei durchbrochen, da TCP-spezifische Information nicht nur in der TCP-Schicht sondern auch in der Netzwerkschicht genutzt wird. Etwaige Veränderungen an TCP erfordern somit ggf. auch Änderungen an den Routern, die in der Netzwerkschicht TCP-Pakete auswerten.

Zwei Verfahren, die in der Schicht 3 operieren, sind in der Literatur beschrieben: Das Filtern von TCP-Paketen und die lokale Wiederholung von TCP-Paketen. Beide Verfahren erfordern keine Modifikationen am Festnetzrechner und erhalten die Ende-zu-Ende-Semantik von TCP. Zusätzliche Statusinformation wird im Router verwaltet. Eine Migrationsunterstützung für diese Statusinformation ist allerdings nur für einen der Ansätze beschrieben. Tabelle 3.3 faßt diese Merkmale zusammen.

Modifikation der Festnetzrechner	TCP Ende-zu-Ende-Semantik	zusätzliche Statusinformation	Migrationssupport für Statusinformation
nicht notwendig	unverändert	notwendig	bedingt notwendig
nicht realisiert			teilweise realisiert

Tabelle 3.3: Klassifikation der betrachteten lokalen Lösungen (Schicht 3)

Filtern von TCP-Paketen
In [CL97] wird zusätzlich zu der in Kapitel 3.2.1.2 beschriebenen Optimierung der timerbasierten Übertragungswiederholung ein Verfahren beschrieben, das von einem TCP-Sender im

Festnetz unnötigerweise wiederholte TCP-Nutzdatenpakete erkennen kann und diese Pakete herausfiltert. Hierzu werden in der Schicht 3 des Routers die TCP-Sequenznummer der TCP-Pakete und die bestätigten Sequenznummern analysiert. Ein TCP-Paket wird herausgefiltert, falls seine Sequenznummer kleiner als die höchste kumulativ bestätigte Sequenznummer ist, die bereits den Router passiert hat. Unnötige Paketübertragungen über einen unter Umständen schmalbandigen drahtlosen Link können somit reduziert werden. Der beschriebene Lösungsansatz ist insbesondere dann von Nutzen, falls TCP Ende-zu-Ende keine selektiven Wiederholungen unterstützt. Lokale Übertragungswiederholungen zwischen dem Router und dem mobilen System, um die höhere Fehleranfälligkeit des drahtlosen Links zu kompensieren, bietet dieser Ansatz nicht.

Lokale Wiederholung von TCP-Paketen
Höhere Bitfehlerraten drahtloser Links adressiert hingegen der an der Universität Berkeley entwickelte *Snoop-Ansatz* [BSK95] durch lokale Übertragungswiederholungen. Hierfür werden analog zu dem im vorangegangenen Abschnitt beschriebenen Verfahren im Router die Paketköpfe von TCP-Paketen analysiert. Auf Basis dieser Information erfolgen ggf. Wiederholungen von TCP-Paketen zwischen dem Router und dem mobilen System. Lokale Übertragungswiederholungen werden sowohl für vom mobilen System gesendete als auch für an das mobile System gesendete TCP-Pakete vorgenommen. Allerdings unterscheiden sich die hierfür notwendigen Mechanismen.

Wie eventuell notwendige Übertragungswiederholungen für an das mobile System adressierte Pakete lokal realisiert werden können, ist in [ABSK95] beschrieben. An das mobile System adressierte TCP-Nutzdatenpakete werden in der Netzwerkschicht des Routers analysiert und für eventuell notwendige Übertragungswiederholungen zwischengespeichert. Aus diesem Zwischenspeicher wird ein Paket erst dann gelöscht, falls ein TCP-Paket, das dieses Paket bestätigt, den Router passiert, und somit das zwischengespeicherte Paket nicht mehr für eine lokale Übertragungswiederholung verfügbar sein muß. Sowohl doppelte TCP-Bestätigungen, die den Router passieren, als auch das Ausbleiben der zum übertragenen TCP-Paket gehörigen Bestätigung wertet der Router als Indiz für einen Paketverlust und veranlaßt eine Übertragungswiederholung. Der zur Überwachung des Empfanges eines Bestätigungspakets im Router verwendete Timer kann mit einem im Vergleich zum TCP-Sender kleineren Timeoutwert initialisiert werden und somit schneller eine Wiederholung des im Zwischenspeicher abgelegten Nutzdatenpakets veranlassen. Um zu vermeiden, daß auf Grund von Bestätigungsduplikaten zusätzlich zu der Übertragungswiederholung des Routers auch mittels Fast Retransmit eine Wiederholung seitens des Senders im Festnetz erfolgt, werden doppelte Bestätigungspakete vom Router herausgefiltert. Ein ähnlicher Ansatz wird in [VMPM99] verfolgt. Die Generierung von Bestätigungsduplikaten wird bei diesem Ansatz im Empfänger eine gewisse Zeit verzögert. Während dieser Zeitdauer können Übertragungswiederholungen, die ggf. nicht reihenfolgetreu erfolgen, in der Schicht 2 vorgenommen werden, ohne daß der TCP-Sender auf Nutzdaten Grund empfangener Bestätigungsduplikate mittels Fast Retransmit wiederholt. Durch einen Timeout beim Sender bedingte Übertragungswiederholungen können beide Ansätze allerdings nicht verhindern.

Beim Snoop-Ansatz werden auch für vom mobilen System gesendete Pakete lokale Übertragungswiederholungen vorgenommen [BSAK95]. Hierzu werden im Router die passierenden TCP-Paket analysiert und durch Übertragungsfehler bedingte Lücken im TCP-Datenstrom erkannt. Mittels negativer Bestätigungen wird das mobile System über diese Lücken informiert

und eine lokale Wiederholung dieser Pakete veranlaßt. Um dieses Verfahren zu realisieren, muß allerdings die TCP-Implementierung des mobilen Systems dahingehend geändert werden, daß es empfangene negative Bestätigungen verarbeiten kann. Diese notwendige Veränderung ist in Abb. 3.3 durch die hellgraue Darstellung der TCP-Schicht des mobilen Systems verdeutlicht.

Migrationsunterstützung

Sowohl der beschriebene Filtermechanismus [CL97] als auch die in der Schicht 3 realisierbaren lokalen Übertragungswiederholungen [BSK95] erfordern die Verwaltung von Statusinformation in den Routern, in denen diese Mechanismen in der Schicht 3 implementiert sind. Die Statusinformation umfaßt die Sequenznummern bestätigter Pakete und die TCP-Pakete, die für etwaige Wiederholungen im Router zwischengespeichert werden müssen.

Auf Grund der Mobilität eines mobilen Systems ändert sich ggf. das Routing der zu diesem bzw. von diesem System gesendeten Pakete. Der Router, der für das Filtern bzw. die lokalen Übertragungswiederholungen verantwortlich war, ist dann ggf. nicht mehr im Datenpfad. In diesem Fall muß ein anderer Router diese Funktion übernehmen. Ohne spezielle Maßnahmen ist allerdings auf diesem Router die TCP-spezifische Statusinformation nicht vorhanden.

Ist diese Statusinformation nicht verfügbar, so ist eine Filterung bzw. eine lokale Übertragungswiederholung in der Schicht 3 des Routers nicht möglich. Diese Mechanismen können somit den Zweck einer verbesserten, effizienteren Datenübertragung über fehleranfällige drahtlose Teilstrecken nicht erfüllen. TCP verhält sich also in diesem Fall so, als ob derartige Mechanismen zur Filterung bzw. lokalen Übertragungswiederholung nicht vorhanden wären. Die Ende-zu-Ende betriebene TCP-Verbindung stellt allerdings sicher, daß trotz eventuell nicht verfügbarer Statusinformation in den Routern eine zuverlässige Kommunikation zwischen dem mobilen System und seinen Kommunikationspartnern im Festnetz möglich ist.

Mechanismen, um die TCP-spezifische Statusinformation auf dem Router verfügbar zu machen, der nach Änderung des Routings die Filterung bzw. die lokalen Übertragungswiederholungen übernimmt, werden für den in [CL97] beschriebenen Ansatz nicht betrachtet.

Der an der Universität Berkeley entwickelte *Snoop-Ansatz* umfaßt hingegen ein Verfahren [SBK97], [Ses95], wie die Statusinformation auf einem anderen Router verfügbar gemacht werden kann, so daß dieser dann ggf. TCP-Pakete lokal wiederholen kann. Beim Snoop-Ansatz wird eine Mobilitätsunterstützung auf Basis von Mobile IP vorausgesetzt. Abweichend von der Mobile IP-Spezifikation werden die Pakete vom Home Agent nicht zur temporären IP-Adresse getunnelt, sondern an eine dem mobilen System zugeordnete Multicast-Adresse gesendet. Dieser Ansatz erfordert eine eigene Multicast-Adresse für jedes unterstützte mobile System. Router, die TCP-Pakete in der Schicht 3 analysieren können und nahe beim mobilen System angeordnet sind, sind potentiell Router, die ggf. nach einem Ortswechsel des mobilen Systems auf der Schicht 3 TCP-Pakete wiederholen können. Treten diese Router frühzeitig der Multicast-Gruppe bei, so kann der Zwischenspeicher bereits mit den ggf. für eine lokale Wiederholung notwendigen TCP-Paketen gefüllt werden. Auch im Falle eines Ortswechsels eines mobilen Systems können dann von diesem Router falls erforderlich – ohne erst die Statusinformation anfordern zu müssen – TCP-Pakete lokal wiederholt werden.

3.3.3 Lösungsansätze in der Schicht 4

Durch fehleranfällige Funkkanäle bedingte Übertragungsfehler können auch durch Übertragungswiederholungen in der Schicht 4, d.h. in der Transportschicht korrigiert werden. Allerdings würde in diesem Falle die Fehlerkorrektur nicht lokal erfolgen, da Protokolle der Schicht 4 Ende-zu-Ende operieren. Grundidee der lokalen Lösungsansätze, die auf der Schicht 4 operieren, aber dennoch lokale Übertragungswiederholungen realisieren, ist es, die Ende-zu-Ende-Transportverbindung in zwei über einzelne Teilstrecken betriebene Verbindungen zu unterteilen. Die Kopplung der Verbindungen erfolgt im sogenannten *Transportgateway* . Anstatt wie bei den bisher beschriebenen Ansätzen Übertragungsfehler des drahtlosen Links lokal auf den Schichten 1-3 zu korrigieren und somit vor den TCP-Instanzen der Endsysteme zu verbergen, wird bei den lokalen Lösungsansätzen der Schicht 4 die TCP-Verbindung vor dem fehleranfälligen drahtlosen Link terminiert. TCP-Instanzen im Festnetz werden deshalb nicht mit den Übertragungseigenschaften drahtloser Links konfrontiert.

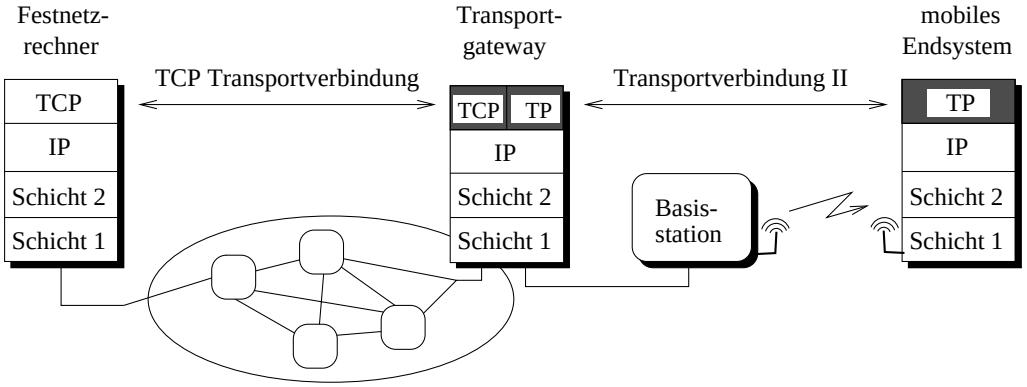


Abbildung 3.4: Der indirekte Transportansatz

Abb. 3.4 zeigt ein Szenario, bei dem die TCP-Verbindung nicht Ende-zu-Ende zwischen dem mobilen System und dem Festnetzrechner besteht. Stattdessen wird die TCP-Verbindung des Festnetzrechners auf einem Transportgateway terminiert, das in der Nähe des mobilen Systems, aber noch vor dem fehleranfälligen drahtlosen Link angesiedelt ist. Zwischen dem Transportgateway und dem mobilen System, wird ein spezielles Transportprotokoll TP verwendet, das auf die Eigenschaften der drahtlosen Übertragung zugeschnitten ist. Da keine direkte Transportverbindung zwischen dem Festnetzrechner und dem mobilen System besteht, wird dieser Ansatz als *indirekter Transportansatz* bezeichnet. In der Literatur werden diese Ansätze auch Proxy-basierte Ansätze genannt. Ein Überblick über diese Ansätze und die bei ihnen auftretenden Probleme ist in [BKG+00] zu finden.

Tabelle 3.4 gibt die wesentlichen Merkmale indirekter Transportansätze wieder. Sie erfordern keine Modifikationen an Festnetzrechnern. Allerdings ergibt sich eine geänderte Ende-zu-Ende-Semantik. Die Realisierung der beiden Transportinstanzen auf einem Transportgateway hat zusätzliche Statusinformation zur Folge. Eine Migrationsunterstützung für diese ist notwendig.

Auf Grund der Terminierung der TCP-Verbindung vor dem drahtlosen Link können sich die in Kapitel 2.3.2 beschriebenen Probleme von TCP beim Einsatz über drahtlosen Teilstrecken nicht ergeben. Um Ende-zu-Ende einen zuverlässigen Dienst zur Verfügung stellen zu können, muß zusätzlich zur mittels TCP realisierten zuverlässigen Kommunikation zwischen

Modifikation der Festnetzrechner	TCP Ende-zu-Ende-Semantik	zusätzliche Statusinformation	Migrationssupport für Statusinformation
nicht notwendig	verändert	notwendig	zwingend notwendig
nicht realisiert			teilweise realisiert

Tabelle 3.4: Klassifikation der betrachteten lokalen Lösungen (Schicht 4)

dem Festnetzrechner und dem Transportgateway auch das zwischen dem Transportgateway und dem mobilen System operierende Transportprotokoll einen zuverlässigen Dienst bieten.

Die Wahl des Transportprotokolls zwischen dem mobilen System und dem Transportgateway hat keinen Einfluß auf die Interoperabilität mit TCP-basierten Kommunikationspartnern im Festnetz. Solange zwischen den Festnetzrechnern und dem Transportgateway TCP als Transportprotokoll verwendet wird, ist die Interoperabilität sichergestellt. Diese Freiheit bezüglich des verwendeten Transportprotokolls zwischen dem Transportgateway und einem mobilen System spiegelt sich auch in den verschiedenen in der Literatur beschriebenen Ansätzen wider, die den indirekten Transportansatz nutzen [Bak96], [SRBW00], [SMA98], [BS97], [HA97], [WT98]. Prinzipiell lassen sich die indirekten Transportansätze in zwei Klassen einteilen. Die Einteilung erfolgt in Abhängigkeit davon, welche Änderungen an den Protokollstacks vorzunehmen sind. Eine Klasse umfaßt die Ansätze, die lediglich zwei zusätzliche Transportinstanzen auf dem Transportgateway realisieren (siehe Abb. 3.4), die andere solche, die tiefgreifendere Änderungen am Protokollstack vornehmen.

Zwei zusätzliche Transportinstanzen auf dem Transportgateway
Gemeinsames Merkmal der in diesem Abschnitt beschriebenen indirekten Ansätze ist, daß der Protokollstack des Transportgateways und des mobilen Systems wie in Abb. 3.4 dargestellt realisiert ist. Abgesehen von den zusätzlich realisierten zwei Transportinstanzen auf dem Gateway und einem speziellen Transportprotokoll zwischen Transportgateway und mobilem System werden keine wesentlichen Veränderungen an den Protokollstacks der Systeme vorgenommen.

Die Idee des indirekten Transportansatzes wurde erstmalig in [BBIM93] vorgestellt. Eine tiefergehende Beschreibung des sogenannten *I-TCP* Ansatzes ist in [BB95b], [Bak96] zu finden. Das Transportprotokoll TCP kommt bei diesem Ansatz nicht nur zwischen dem Festnetzrechner und dem Transportgateway zum Einsatz, sondern wird auch für die Kommunikation zwischen dem Transportgateway und dem mobilen System eingesetzt. Durch Bitfehler oder Unterbrechungen des Funkkanals bedingte Paketverluste haben somit auf Grund von Lastreduktionen Durchsatzeinbußen der TCP-Verbindung zwischen dem Transportgateway und dem mobilen System zur Folge. Da im Vergleich zur Ende-zu-Ende-Übertragung die Paketumlaufzeit allerdings geringer ist, wird das Lastkontrollfenster wieder schneller geöffnet und Übertragungsfehler werden schneller korrigiert. Aus diesen Gründen ergibt sich insgesamt eine Performancesteigerung im Vergleich zum Ende-zu-Ende betriebenen TCP.

Yavatkar und Bhagawat [YB94] schlagen ebenfalls vor, einen indirekten Transportansatz zu verwenden. Um durch die höhere Fehlerrate des drahtlosen Links bedingte Übertragungsfehler schneller und effizienter korrigieren zu können, werden bei diesem Verfahren zusätzlich selektive Bestätigungen und Übertragungswiederholungen in dem über der drahtlosen Teilstrecke verwendeten Transportprotokoll verwendet.

Auch in [HA97] wird ein spezielles Transportprotokoll, das sogenannte *Mobile-TCP*, für die Übertragung zwischen dem Transportgateway und dem mobilen System beschrieben. Hauptaugenmerk liegt hierbei darauf, den Aufwand für die Transportprotokollverarbeitung auf dem mobilen System auf Kosten eines erhöhten Protokollaufwandes im Transportgateway zu verringern. Diese Asymmetrie hinsichtlich des Protokollverarbeitungsaufwandes adressiert somit weniger leistungsfähige mobile Systeme und Systeme, bei denen der für die Kommunikation erforderliche Anteil der Akkukapazität verringert werden soll. Obwohl eine Migrationsunterstützung notwendig ist, wird von den Autoren auf diese nicht eingegangen.

Der indirekte *M-TCP* Transportansatz [BS97], [Bro97] von Brown und Singh adressiert kurze und lange Unterbrechungen des Funkkanals. Es wird davon ausgegangen, daß das zwischen dem Transportgateway und dem mobilen System operierende Transportprotokoll nicht mit einer höheren Paketfehlerrate konfrontiert wird, da bereits Schicht 2 Wiederholungen die Übertragungsfehler korrigieren. Die Transportschicht wird somit lediglich mit höheren Schwankungen der Paketumlaufzeit konfrontiert. Herausragendes Merkmal des M-TCP Ansatzes im Vergleich zu anderen indirekten Ansätzen ist, daß trotz der Unterteilung der Ende-zu-Ende-Transportverbindung in zwei Verbindungen die Semantik der Bestätigungen unverändert bleibt. Dies wird erreicht, indem die Transportinstanz im Transportgateway eine Bestätigung an das sendende Endsystem für ein korrekt empfangenes Nutzdatenpaket solange verzögert, bis das Transportgateway durch eine Bestätigung vom empfangenden Endsystem über den korrekten Empfang informiert wurde. Sowohl Unterbrechungen des Funkkanals als auch die beschriebene Verzögerung der Generierung einer Bestätigung beim Transportgateway können beim sendenden Endsystem Timeouts und unnötige Lastreduktionen zur Folge haben. Die Timeouts werden vom M-TCP Ansatz vermieden, indem der TCP-Sender vor dem Timerablauf in den sogenannten Persist-Modus von TCP versetzt wird. In diesem Modus werden die Timer eingefroren. Deshalb können Timeouts und Lastreduktionen vermieden werden. Ein Wechsel in den Persist-Modus wird vom Transportgateway veranlaßt.

Ein Transportgateway wird auch in dem in [MB98] beschriebenen *MSOCKS*-Ansatz eingesetzt. Im Gateway werden allerdings lediglich die IP-Adressen, Portnummern und Sequenznummern der Transportprotokollpakete modifiziert. Ziel des Ansatzes ist, es Anwendungen zu ermöglichen, die IP-Adresse, d.h. den verwendeten Kommunikationsendpunkt zu wechseln, während die Kommunikation aktiv ist. Die dann erforderliche Adreßumsetzung wird im Gateway vorgenommen. Da keine weitergehende Protokollverarbeitung im Gateway erfolgt und insbesondere die Übertragungseigenschaften der drahtlosen Strecke nicht lokal adressiert werden, d.h. sich Ende-zu-Ende auswirken, wird auf diesen Ansatz nicht weiter eingegangen. Er ist lediglich der Vollständigkeit wegen mit aufgeführt.

Tiefgreifendere Änderungen am Protokollstack

Die in [KRL+97], [SMA98], [SRBW00], [WT98] beschriebenen Ansätze für die Umsetzung des indirekten Ansatzes erfordern tiefergreifende Veränderungen der Protokollstacks der involvierten Systeme.

In [AKLR97], [KRL+97] und [SMA98] wird vorgeschlagen, in dem Gateway nicht nur die Kopplung der Transportprotokolle vorzunehmen, sondern auch Funktionalität höherer Protokollschichten zu realisieren. Beispielsweise ist eine Nutzdatenkomprimierung oder eine Modifikation der Anwendungsdaten im Gateway – wie z.B. in WAP [Dul00] – denkbar.

Tiefgreifendere Veränderungen an den Protokollstacks der mobilen Systeme werden auch

in [WT98], [SRBW00] vorgenommen. Gemeinsames Merkmal dieser beiden Ansätze ist das Fehlen der TCP-Schicht und der IP-Schicht in den mobilen Systemen. TCP-Verbindungen der Festnetzrechner werden auf dem Gateway terminiert und ein eigenes Protokoll für die Übertragung der Nutzdaten zum mobilen System verwendet. In der an der TU Berlin entwickelten *Remote Socket Architecture* [SRBW00] wird vorgeschlagen, TCP-Verbindungen zum mobilen System auf der Basisstation zu terminieren. Der TCP/IP-Protokollstack ist auf der Basisstation implementiert. Socket-Aufrufe [WS95] einer Anwendung auf dem mobilen System werden mittels eines zuverlässigen Übertragungsdienstes zur Basisstation übermittelt. Dort werden die Nutzdaten an die jeweilige TCP-Instanz übergeben bzw. von dieser übernommen. Da die Basisstation und das mobile System unmittelbar benachbart sind, ist ein zuverlässiges sogenanntes Last Hop Protocol ausreichend. Dieser Ansatz erlaubt es allerdings nicht, die TCP-Verbindung auf einem anderen System als der Basisstation zu terminieren, da ansonsten zusätzlich zum Last Hop Protocol Routing-Aspekte mit berücksichtigt werden müssen. Einen ähnlichen Ansatz, TCP/IP auf der Basisstation zu terminieren und ein zuverlässiges Schicht 2 Protokoll zwischen dem Gateway und dem mobilen System zu verwenden, ist in [WT98] beschrieben. Das entwickelte Protokoll *METP* (Mobile End Transport Protocol) bietet diese Zuverlässigkeit. Auch bei diesem Ansatz ist es nicht möglich, die TCP-Verbindung auf einem anderen System als der Basisstation zu terminieren.

Migrationsunterstützung

Wie bei den in Kapitel 3.3.2 beschriebenen Lösungsansätzen in der Schicht 3 wird auch bei der Umsetzung des indirekten Transportansatzes TCP-spezifische Statusinformation in dem Router verwaltet, der als Transportgateway fungiert. Für den Betrieb eines indirekten Transportansatzes muß die Statusinformation beim Transportgateway verfügbar sein. Andernfalls ist auf der Transportebene keine Kommunikation zwischen dem mobilen System und seinem Kommunikationspartner im Festnetz möglich. Bei den Schicht 3 Ansätzen kann hingegen auch im Falle fehlender TCP-Statusinformation im Router Ende-zu-Ende kommuniziert werden. Das Fehlen der Statusinformation hat lediglich zur Folge, daß die in der Schicht 3 angesiedelten Mechanismen zur Optimierung der Übertragung über fehleranfälligen Funkkanälen nicht einsetzbar sind.

Da die indirekten Transportansätze zwingend die Verfügbarkeit der Statusinformation in dem Router erfordern, der aktuell als Transportgateway fungiert, muß dies durch geeignete Maßnahmen sichergestellt werden. Es ist zwingend erforderlich, daß das aktive Transportgateway immer, d.h. auch nach Ortswechseln des mobilen Systems, im Datenpfad liegt. Ist das nicht der Fall, so muß ein neues Transportgateway die Funktion des nun nicht mehr im Datenpfad liegenden Gateways übernehmen. Erst nachdem auf dem neuen Gateway die Statusinformation vorhanden ist, kann dieses als Transportgateway für die jeweilige indirekte Transportverbindung fungieren. Die Übertragung der Statusinformation vom alten Transportgateway zum neuen Transportgateway wird als *Migration der Statusinformation* bezeichnet.

[HA97], [SMA98], [SMA98] beschreiben Lösungsansätze unter Verwendung des indirekten Transportansatzes, adressieren aber nicht das Problem der Migration der Statusinformation. Der Einsatz des indirekten Transportansatzes bleibt deshalb bei diesen Ansätzen auf stationäre bzw. portable Endsysteme beschränkt, mobile Endsysteme können nicht unterstützt werden. In [BB95a], [Bro97] und [WT98] wird auf die Migration von Transportinstanzen eingegangen. Sie werden in Kapitel 3.5, in dem der Stand der Forschung beim indirekten Transportansatz beschrieben wird, detaillierter vorgestellt.

3.4 Vergleich und Bewertung der Ansätze

Die in den Unterkapiteln 3.2 und 3.3 beschriebenen Lösungsansätze werden im folgenden dahingehend bewertet, inwieweit sie die im Rahmen der vorliegenden Arbeit gestellten Anforderungen erfüllen können. Es sind dies die bereits in Kapitel 1.1 formulierten und eine zusätzliche Anforderung:

- Keine Modifikation der TCP-Implementierung in den Festnetzrechnern,
- Berücksichtigung von Unterbrechungen und höheren Bitfehlerraten,
- Integration mit der Mobilitätsunterstützung im Internet auf Basis von Mobile IP und
- Einsatz über drahtlosen Netzen mit bzw. ohne Schicht 2 Wiederholungen.

Die letzte angeführte Anforderung ist in die Liste der Anforderungen mit aufgenommen, da zumindest kurzfristig bis mittelfristig davon auszugehen ist, daß sowohl drahtlose Netze, die Übertragungswiederholungen auf der Schicht 2 einsetzen, als auch Netze, die auf diese verzichten, am Markt verfügbar sein werden. Ein universell einsetzbarer Lösungsansatz muß somit sowohl mit signifikanten Schwankungen der Paketumlaufzeit (Schicht 2 Wiederholungen realisiert) als auch mit höheren Paketfehlerraten (keine Wiederholungen in der Schicht 2) zurechtkommen.

In Tabelle 3.5 ist dargestellt, inwieweit die genannten Anforderungen von den verschiedenen Lösungsansätzen adressiert werden. Zusätzlich ist in die Tabelle mit aufgenommen, von welchem System Übertragungswiederholungen vorgenommen werden, falls Übertragungsfehler auf der drahtlosen Teilstrecke dies erfordern. Darüber hinaus kann der Tabelle entnommen werden, ob der jeweilige Ansatz die Verwaltung zusätzlicher Statusinformation innerhalb des Netzwerkes erfordert und ob der Ansatz eine Migrationsunterstützung für diese Statusinformation umfaßt. Das Transportprotokoll, dessen Transportprotokolldateneinheiten über der drahtlosen Teilstrecke übertragen werden, ist in der letzten Spalte der Tabelle aufgeführt.

Ende-zu-Ende-Lösungsansätze
Ein wesentlicher Vorteil der Ende-zu-Ende-Lösungen ist, daß ihr Nutzen nicht auf mobile Systeme beschränkt ist. Von einer schnelleren Fehlerkorrektur nach Übertragungsfehlern und der Vermeidung einer Lastreduktion nach durch Bitfehlern bedingten Paketverlusten profitieren auch Systeme, die nicht drahtlos angebunden sind. Darüber hinaus ist nicht wie bei anderen Ansätzen die Verwaltung und ggf. die Migration von zusätzlicher Statusinformation im Netzwerk erforderlich. Ein wesentlicher Nachteil ist darin zu sehen, daß Änderungen an Protokollstacks von Rechnern, die im Festnetz installiert sind, nur schwer umzusetzen sind. Darüber hinaus ist die Modifikation der Lastkontrollmechanismen von TCP – zum Beispiel die Verwendung expliziter Signale – problematisch, da die Lastkontrolle eine zentrale Komponente zur Vermeidung und Behebung von Überlastsituationen darstellt. Eine Fehlfunktion hätte dramatische Auswirkungen zur Folge. Im Vergleich zu den vorgestellten lokalen Übertragungswiederholungen ist die Ende-zu-Ende-Korrektur von Übertragungsfehlern langsamer und aus diesem Grund nicht zu favorisieren. Weiterhin bieten Ende-zu-Ende-Lösungen nicht die Möglichkeit, wie lokale Lösungen die aktuellen Übertragungsbedingungen der fehleranfälligen Übertragungsstrecke mit zu berücksichtigen. Beispielsweise ist es Ende-zu-Ende-Lösungen

Ende-zu-Ende TCP Tranportverbindung	Modifikation des TCP Protokoll-stacks in den Endsystemen	TCP-Sack	End-system	ja	ja	nein	nein	nein	nein	TCP
		TCP-Zeit-stempel	End-system	ja	ja	nein	nein	nein	nein	TCP
		Auxiliary Timeout	End-system	ja	ja	nein	nein	nein	nein	TCP
		künstliches Fast Retrans.	End-system	nein	nein	ja	nein	nein	nein	TCP
		Explizite Feedbacksignale	End-system	ja	nein	ja	nein	nein	nein	TCP
		TCP-Eifel	End-system	ja	nein	ja	ja	nein	nein	TCP
indirekte Transportverbindung	Lokale Lösungen Schicht 2	channel state dependent scheduling	Basis-station	nein	nein	ja	nein	ja	nein	TCP
		Paketlängen-anpassung	keine	nein	ja	nein	nein	nein	nein	TCP
		Schicht 2 Wiederholungen	Basis-station	nein	ja	nein	-	ja	nein	TCP
	Lokale Lösungen Schicht 3	Filterung	keine	nein	nein	nein	nein	ja	nein	TCP
		Snoop	Router	nein	ja	nein	nein	ja	ja	TCP NACK
	Lokale Lösungen Schicht 4	Remote Sockets	Basis-station	nein	ja	ja	ja	ja	nein	kein TP
		I-TCP	Gate-way	nein	ja	nein	nein	ja	ja	TCP
		M-TCP	Gate-way	nein	nein	ja	ja	ja	ja	mod. TCP
		Mobile TCP	Gate-way	nein	nein	ja	nein	ja	nein	eigenes
		Indirekter Ansatz mit OMIT	Gate-way	nein	ja	ja	nein	ja	ja	eigenes möglich

Tabelle 3.5: Aufstellung der verschiedenen Lösungsansätze

nicht möglich, die zu verwendende Paketlänge auf die aktuellen Übertragungseigenschaften des Funkkanals abzustimmen.

Da sich die in Tabelle 3.5 aufgeführten Lösungsansätze 'TCP-Sack' und 'TCP-Zeitstempel' zunehmend in aktuellen Protokollstacks etablieren (siehe Kapitel 3.2.1.1), kann das Argument,

daß ein langfristiger Einführungsprozeß dieser Mechanismen in die Protokollstacks der Festnetzrechner gegen diese Ansätze spricht, nicht angeführt werden. Trotzdem sind diese Ansätze nur bedingt hilfreich, da sie das sich durch stärkere Schwankungen der Paketumlaufzeit ergebende Problem unnötiger TCP-Timeouts mit anschließender unnötiger Lastreduktion nicht lösen. Gegen die Lösungsansätze 'Auxiliary Timeout', 'Explizite Lastkontrolle' und 'TCP-Eifel' sprechen die hierfür notwendigen Änderungen an den Protokollstacks der installierten Festnetzrechner. Der Ansatz 'künstliches Fast Retransmit' erfordert zwar nur Änderungen am mobilen System und ermöglicht eine schnelle Wiederaufnahme der Kommunikation auf der Transportebene nach längeren Unterbrechungen des Funkkanals. Ein wesentlicher Nachteil dieses Lösungsansatzes ist aber, daß er zwar eine schnelle Wiederaufnahme der Kommunikation ermöglicht, nach Wiederaufnahme der Kommunikation das Lastkontrollfenster aber nur langsam geöffnet wird. Wegen wiederholter Paketverluste während der Unterbrechung wird der Slow-Start-Grenzwert auf 2 reduziert (siehe Kapitel 2.3.2.1, Abb. 2.16). Deshalb ist bei Wiederaufnahme der Kommunikation die Phase der exponentiellen Öffnung des Lastkontrollfensters sehr kurz. Die stattdessen vorgenommene langsame lineare Öffnung hat unnötige Durchsatzeinbußen zur Folge.

Eine Reduktion des Slow-Start-Grenzwertes auf den Wert 2 ergibt sich zwangsläufig nach mehreren aufeinanderfolgenden Timeouts, beispielsweise bedingt durch Unterbrechungen des Übertragungskanals. Diese Reduktion läßt sich nur vermeiden, indem die TCP-Implementierung des Senders entsprechend modifiziert wird. Da Änderungen der TCP-Implementierungen von Festnetzrechnern im Rahmen der vorliegenden Arbeit als nicht praktikabel angesehen werden, kann mittels Ende-zu-Ende-Lösungsansätzen die Reduktion des Slow-Start-Grenzwertes nach längeren Unterbrechungen auf den Minimalwert nicht vermieden werden. Aus diesem Grunde werden Ende-zu-Ende-Lösungsansätze im Rahmen dieser Arbeit nicht weiter betrachtet.

Lokale Lösungsansätze in der Schicht 2

Vorteil der in der Schicht 2 angesiedelten Lösungsansätze ist es, daß sie Kenntnisse hinsichtlich der aktuellen Übertragungseigenschaften des Funkkanals in die Entscheidung, welche Mechanismen zur Kompensation des fehleranfälligen Links zum Einsatz kommen, mit einfließen lassen können. Es sind dies die folgenden auch in Tabelle 3.5 aufgeführten Mechanismen: 'channel state dependent scheduling', 'Paketlängenanpassung' und 'Schicht 2 Wiederholungen'. Kommen Übertragungswiederholungen zum Einsatz, so sind diese lokaler Natur, d.h. es werden keine Ressourcen des Festnetzes hierfür verbraucht. Ein weiterer Vorteil ist darin zu sehen, daß für den Einsatz dieser Mechanismen keine Veränderungen an den Systemen im Festnetz erforderlich sind.

Problematisch bei Ansätzen in der Schicht 2 ist, daß sie zwar Übertragungsfehler auf Kosten zusätzlicher Delays korrigieren können, diese zusätzlichen Delays in den TCP-Instanzen der Endsysteme aber ggf. Probleme nach sich ziehen. Desweiteren lassen sich Auswirkungen langer Unterbrechungen eines Funkkanals nicht vor den Endsystemen verbergen. Die durch die Reduktion des Slow-Start-Grenzwertes auf den Wert 2 bedingten Durchsatzeinbußen, die bereits bei der Diskussion der Ende-zu-Ende-Lösungsansätze beschrieben sind, können auch durch Schicht 2 Lösungen nicht vermieden werden.

Trotzdem sind die Schicht 2 Mechanismen als sinnvoll einsetzbar anzusehen, insbesondere da sie die Probleme an der Wurzel angehen, d.h. lokal zu beheben versuchen. Ihr alleiniger

Einsatz ist allerdings nicht ausreichend. Zusätzlich sind Mechanismen in höheren Schichten des Protokollstacks erforderlich, um mit längeren Unterbrechungen und durch Übertragungswiederholungen in der Schicht 2 verursachten Schwankungen der Paketumlaufzeit zurechtzukommen.

Lokale Lösungsansätze in der Schicht 3
Den in Tabelle 3.5 dargestellten Lösungsansätzen der Schicht 3 ist gemeinsam, daß sie TCP-Pakete auswerten und somit genauere Kenntnis über die Aktionen der TCP-Instanzen der Endsysteme erlangen. Da sowohl die TCP-Instanzen der Endsysteme als auch die lokalen, im Router ergriffenen Maßnahmen auf TCP-Paketen operieren, läßt sich ein besseres Zusammenspiel als mit den Lösungsansätzen der Schicht 2 erreichen. Das Zusammenspiel der Schicht 3 Mechanismen mit den TCP-Mechanismen bietet einerseits zwar Vorteile, hat zum anderen aber auch den Nachteil, daß lediglich TCP-basierte Datenströme von den Änderungen profitieren können.

Der 'Filterungs-Ansatz', der in Tabelle 3.5 aufgeführt ist, macht nur dann Sinn, falls häufiger wiederholte, d.h. identische TCP-Pakete den Router passieren. Dies ist der Fall, falls TCP mittels Go-Back-N Pakete wiederholt. Da aber zunehmend selektive Bestätigungen und selektive Wiederholungen in TCP-Implementierungen Einzug erhalten (siehe Kapitel 3.2.1.1), ist von dem Filtermechanismus kein großer Nutzen zu erwarten.

Der 'Snoop-Ansatz' ist nicht gewinnbringend einsetzbar, falls das drahtlose Netz bereits Schicht 2 Wiederholungen unterstützt, da dann Wiederholungen in der Schicht 3 nicht mehr erforderlich sind. Für drahtlose Netze ohne Schicht 2 Wiederholungen ist es hingegen in Grenzen möglich, Übertragungsfehler vor den TCP-Instanzen der Endsysteme zu verbergen. Dies gelingt nur dann, wenn der TCP-Timer im Sender so konservativ gewählt ist, daß für die Übertragungswiederholung genügend Zeit verbleibt.

Der Snoop-Ansatz bietet nicht die Möglichkeit, gezielt Wissen über den aktuellen Zustand des Übertragungskanals zu nutzen. Weiterhin ergibt sich beim Snoop-Ansatz das Problem, daß längere Unterbrechungen und durch Übertragungswiederholungen bedingte zusätzliche Ende-zu-Ende-Verzögerungen nicht vor dem Sender verborgen werden können. Wie bei den in der Schicht 2 operierenden Lösungsansätzen hat auch beim Snoop-Ansatz eine längere Unterbrechung eine Reduktion des Slow-Start-Grenzwertes auf den Wert 2 und somit drastische Durchsatzeinbußen zur Folge. Aus den genannten Gründen kann diese Klasse von Lösungsansätzen die im Rahmen der vorliegenden Arbeit gestellten Anforderungen nicht erfüllen und wird deshalb nicht weiter verfolgt.

Lokale Lösungsansätze in der Schicht 4
Gemeinsames Merkmal der in Tabelle 3.5 aufgelisteten lokal operierenden Lösungsansätze in der Schicht 4 ist, daß sie zur Gruppe der indirekten Transportansätze gehören. Die Partnertransportinstanz des Festnetzrechners, mit dem das mobile System kommuniziert, ist nicht auf dem mobilen System, sondern auf dem Transportgateway realisiert. Die TCP-Instanz des Festnetzrechners wird deshalb nicht mit erfolglosen Übertragungen von Nutzdatenpaketen konfrontiert, die durch Bitfehler oder Unterbrechungen der drahtlosen Übertragung bedingt sind. Somit kann auch im Fall längerer Unterbrechungen eine Reduktion des Slow-Start-Grenzwertes auf den Minimalwert 2 vermieden werden. Änderungen an den TCP-Instanzen

der Festnetzrechner sind nicht notwendig. Das Transportprotokoll zwischen dem Transportgateway und dem mobilen System kann so konzipiert werden, daß es kurze bzw. lange Unterbrechungen adressiert. Darüber hinaus sollte das Transportprotokoll sowohl durch Bitfehler bedingte Paketverluste korrigieren können, als auch mit Schwankungen der Paketumlaufzeit zurechtkommen, die durch Wiederholungen in der Schicht 2 verursacht werden. Die in der vorliegenden Arbeit gestellten Anforderungen lassen sich somit erfüllen, falls in dem Transportprotokoll zwischen Transportgateway und dem mobilen System hierfür geeignete Mechanismen realisiert sind.

Beim 'Remote Socket' Ansatz ist im mobilen Endsystem kein TCP/IP-Protokollstack implementiert. Daher kann die im Rahmen der vorliegenden Arbeit gestellte Anforderung, die Mobilitätsunterstützung auf Basis von Mobile IP zu realisieren, für diesen Ansatz nicht umgesetzt werden. Der 'Remote Socket' Ansatz wird im folgenden nicht weiter betrachtet. Der 'I-TCP' Ansatz verwendet zwischen dem Transportgateway und dem mobilen System das TCP-Protokoll. Er adressiert Unterbrechungen nicht angemessen, da sich die bereits bei den Ende-zu-Ende-Lösungsansätzen beschriebenen Probleme bzgl. der Lastkontrolle von TCP ergeben. Der 'M-TCP' Ansatz setzt voraus, daß in der Schicht 2 Wiederholungen realisiert werden. Ohne diese Wiederholungen kann er nicht eingesetzt werden. Der 'Mobile-TCP' Ansatz adressiert die höhere Bitfehlerrate nicht angemessen.

Gemeinsames Manko der Ansätze ist die Migrationsunterstützung für die Statusinformation. Der 'Remote Socket' Ansatz und der 'Mobile-TCP' Ansatz bieten für die Migrationsunterstützung keine geeigneten Lösungen. Für den 'I-TCP' Ansatz und den 'M-TCP' Ansatz werden zwar Lösungsvorschläge gemacht, diese erweisen sich aber auf Grund der sich ergebenden Unterbrechungen nur als bedingt geeignet.

Da der indirekte Transportansatz unter Berücksichtigung der in der vorliegenden Arbeit zugrundegelegten Anforderungen als einziger – ohne Änderungen an den TCP-Instanzen der Festnetzrechner – auch im Fall längerer Unterbrechungen eine Reduktion des Slow-Start-Grenzwertes auf den Minimalwert 2 vermeiden und somit Unterbrechungen angemessen adressieren kann, wird er im folgenden Unterkapitel eingehender betrachtet. Es werden offene Probleme im Kontext des indirekten Transportansatzes diskutiert.

3.5 Der Indirekte Transportansatz im Detail

In diesem Kapitel wird auf im Kontext des indirekten Transportansatzes auftretende Probleme eingegangen und es wird diskutiert, wie gravierend diese Probleme sind bzw. welche Lösungen verfügbar sind. Die Betrachtungen zeigen, daß die Migrationsunterstützung ein zentrales ungelöstes Problem darstellt. Auf sie wird eingegangen, existierende Migrationskonzepte werden skizziert und Schwachpunkte dieser Konzepte identifiziert. Die Beschreibung eines besser geeigneten Konzeptes für die Migrationsunterstützung folgt in Kapitel 4.

3.5.1 Spezielle Transportprotokolle

Welche Protokollmechanismen in dem Transportprotokoll zwischen dem Transportgateway und dem mobilen System realisiert werden, wird im Rahmen dieser Arbeit nicht weiter betrachtet. Die Auswirkungen der jeweiligen realisierten Transportprotokollmechanismen sind

lokaler Art, d.h. sie haben keinen Einfluß auf die Verbindung zwischen dem Transportgateway und dem Festnetzrechner, mit dem das mobile System kommuniziert. Hinsichtlich möglicher, auf den jeweiligen Einsatzzweck zugeschnittener Transportprotokolle sei auf die in Kapitel 3.3.3 aufgeführten Ansätze und Protokolle verwiesen. Eigene Arbeiten bzgl. geeigneter Transportprotokollmechanismen, die höhere Fehlerraten und größere durch Übertragungswiederholungen in der Schicht 2 bedingte Schwankungen der Paketumlaufzeit adressieren, sind in [ZF96], [FZ97c] beschrieben.

Unabhängig vom konkret zwischen dem Transportgateway und dem mobilem System realisierten Transportprotokoll werden in der Literatur eine Reihe von Problemen genannt, die gegen die Verwendung des indirekten Transportansatzes sprechen. Eine größere Akzeptanz indirekter Transportansätze läßt sich nur dann erreichen, falls für diese Probleme Lösungen gefunden werden oder Argumente die Relevanz dieser Probleme widerlegen.

3.5.2 Ungelöste Probleme des indirekten Ansatzes

Die Gründe, die gegen die Verwendung indirekter Transportansätze angeführt werden, werden im folgenden nacheinander aufgegriffen. Es wird erläutert, warum diese Gründe nur bedingt geeignet sind, um gegen die Verwendung indirekter Ansätze zu argumentieren.

Ende-zu-Ende-Semantik
Als Nachteil indirekter Transportansätze wird häufig die im Vergleich zu Ende-zu-Ende-Ansätzen geänderte Semantik von Bestätigungspaketen des Transportprotokolls angeführt. Im Fall eines Ende-zu-Ende-Transportprotokolls besagt ein beim Sender eintreffendes Bestätigungspaket, daß das bestätigte Paket erfolgreich zur Transportinstanz des Endsystems übertragen wurde. Im Fall des indirekten Ansatzes bedeutet der Empfang des Bestätigungspakets lediglich, daß das bestätigte Paket zum Transportgateway übertragen wurde. Über den korrekten Empfang des Transportprotokollpakets seitens des Endsystems wird der Sender hingegen nicht informiert.

Aus Sicht der Transportinstanz ist es korrekt, von einer geänderten Semantik der Bestätigungen zu sprechen. Die Schnittstelle zwischen Anwendung und Transportinstanz auf dem Sender ermöglicht es allerdings nicht, die Anwendung darüber zu informieren, wann und ob die zuverlässig zu übertragenden Daten korrekt vom Kommunikationspartner empfangen wurden. Aus diesem Grunde macht es für die Anwendung beim Sender keinen Unterschied, ob empfangene Bestätigungspakete des Transportprotokolls eine erfolgreiche Übertragung der Pakete zum Transportgateway oder zum Endsystem bedeuten.

Für den 'Remote Socket' Ansatz wird in [SRBW00] bzgl. der Ende-zu-Ende-Semantik analog argumentiert: Da es das Socket-Interface [WS95] nicht erlaubt, die Anwendung im Sender über eine erfolgreiche Übertragung der Nutzdaten zu informieren, ist es nicht relevant, ob TCP-Bestätigungen vom Proxy (Transportgateway) oder vom Endsystem generiert werden.

Weil sich aus Sicht der Anwendung durch die geänderte Semantik der Bestätigungen der Transportschicht keine Änderungen ergeben, erscheint es fragwürdig, die geänderte Semantik als Argument gegen den indirekten Ansatz anzuführen.

Verschlüsselung
Wird IPsec [KA98] eingesetzt, so werden die Nutzdaten eines IP-Pakets Ende-zu-Ende verschlüsselt. Im Transportgateway kann somit nicht auf den Transportprotokollkopf der Pakete zugegriffen werden und somit auch keine Transportprotokollverarbeitung erfolgen. Der indirekte Transportansatz kann aus diesem Grunde nicht zusammen mit einer Ende-zu-Ende-Verschlüsselung realisiert werden.

Ein in [ZS00] vorgeschlagenes Verfahren für die Verschlüsselung von IP-Paketen ermöglicht es, Verschlüsselung zusammen mit dem indirekten Ansatz einzusetzen. Die Verschlüsselung eines IP-Pakets erfolgt in mehreren Schichten. Paketköpfe, die für die Protokollverarbeitung im Transportgateway zugänglich sein müssen, werden in einer Schicht verschlüsselt, die Nutzdaten Ende-zu-Ende in einer weiteren Schicht. Indem die Entschlüsselung der Paketköpfe im Transportgateway unterstützt wird, kann dieses Verfahren zusammen mit dem indirekten Ansatz eingesetzt werden.

Eine Alternativlösung wäre es, nicht in der IP-Schicht zu verschlüsseln, sondern durch Verschlüsselung in der Anwendungsschicht die Nutzdaten vor unbefugtem Zugriff zu sichern. Damit wäre der Zugriff auf die Protokollköpfe im Transportgateway möglich. Eine unverschlüsselte Übertragung der Protokollköpfe ist auch erforderlich, um in Routern für eine QoS-Unterstützung einzelne Datenströme identifizieren zu können.

Die skizzierten Verfahren ermöglichen es, auch für indirekte Ansätze eine Verschlüsselung zu realisieren. Das Argument, indirekte Ansätze ließen sich prinzipiell nicht zusammen mit Verfahren für die Verschlüsselung der Daten einsetzen, erscheint somit fragwürdig.

Skalierbarkeit & Performance
Da in einem Transportgateway für jedes Paket zusätzlich zur Protokollverarbeitung in der IP-Schicht auch Protokollverarbeitung in der Transportschicht notwendig ist, stellt der indirekte Transportansatz höhere Anforderungen an die Rechenleistung. Es stellt sich die Frage, inwieweit durch das Transportgateway zusätzliche Delays die Folge sind. Weiterhin ist zu betrachten, für wieviele indirekte Transportverbindungen ein Zwischensystem als Transportgateway operieren kann, d.h. inwieweit der Ansatz skaliert.

In den in [MB98] beschriebenen Untersuchungen wird ein Pentium 200 Mhz Rechner als Transportgateway eingesetzt und untersucht, welchen zusätzlichen Delay die Realisierung eines Transportgateways zur Folge hat. Die gemessenen zusätzlichen Verzögerungen sind kleiner als 1 ms. Weiterhin zeigen die Untersuchungen, daß das Transportgateway für ca. 100 Verbindungen als Transportgateway operieren kann, ohne daß die Protokollverarbeitung zum Engpaß wird. Unter Annahme von einer Datenrate von 2 Mbit/sec pro Verbindung ergibt sich eine aggregierte Bandbreite von 200 Mbit/sec, für die das Zwischensystem als Transportgateway ausreichend Ressourcen bietet. Ähnliche Untersuchungen für einen 100 Mhz Rechner als Transportgateway sind in [BS97], [Bro97] beschrieben. Die aggregierte Bandbreite der indirekten Verbindungen, für die die Ressourcen des Zwischensystems ausreichen, um als Transportgateway zu operieren, wird mit 100 Mbit/sec angegeben.

Die genannten Messungen zeigen, daß ein Router zwar für einige 100 indirekte Verbindungen als Transportgateway fungieren kann, sie belegen aber zugleich, daß zentrale Router auf Grund der um Größenordnungen höheren Anzahl an Verbindungen nicht als Zwischensysteme in Frage kommen, auf denen Transportgateways realisiert werden können. Stattdessen muß ein Transportgateway gezielt auf weniger zentralen Routern plaziert werden. Die im Rahmen

der vorliegenden Arbeit entwickelten Konzepte berücksichtigen dies. Sogenannte *Edge-Router* sind Kandidaten, um auf diesen Transportgateways zu realisieren.

Darüber hinaus ist es vorstellbar, analog zu aktive Netze Konzepten, die zum Teil ebenfalls komplexe Operationen auf den Datenströmen realisieren wollen, diese rechenintensiven Operationen auf Hardware auszulagern [MHWZ99], [TSS+97], [CKV+99].

Migration von Transportinstanzen
Eine Migrationsunterstützung ist erforderlich, um die Transportinstanzen auf ein anderes Transportgateway zu migrieren. Dies ist auf Grund der Mobilität der Endsysteme notwendig (siehe Seite 71). Die Migrationsunterstützung macht die Statusinformation der Transportinstanzen auf einem anderen Transportgateway verfügbar. Das zentrale Problem im Kontext der Migration sind die durch die Migration bedingten Unterbrechungen und die Häufigkeit dieser Unterbrechungen.

- Dauer der durch eine Migration bedingten Unterbrechungen
  Das in [BB95a] beschriebene Verfahren zur Migration von Transportinstanzen hat eine Unterbrechungsdauer der Kommunikation in der Transportschicht von bis zu 1.4 Sekunden zur Folge. Diese Unterbrechungsdauer wird als Argument gegen den indirekten Transportansatz angeführt. Die Unterbrechungsdauer zu reduzieren ist eine Zielsetzung der vorliegenden Arbeit.

- Häufigkeit der Migration
  Wird wie in [BB95b] das Transportgateway auf der Basisstation realisiert, so ergibt sich bei jedem Basisstationswechsel die Notwendigkeit, die Transportinstanzen vom Transportgateway auf der alten zum Transportgateway auf der neuen Basisstation zu migrieren. Sehr häufige Migrationen können die Folge sein. Derart häufige Migrationen zu vermeiden, ist ein weiteres Ziel der in der vorliegenden Arbeit entwickelten Verfahren.

3.5.3 Migration von Transportinstanzen

Die Ausführungen des vorangegangenen Unterkapitels zu den Problembereichen Ende-zu-Ende-Semantik, Verschlüsselung und Skalierbarkeit zeigen, daß diese Probleme entweder von geringer Relevanz sind oder aber durch die skizzierten Ansätze gelöst werden können. Die Migration von Transportinstanzen ist dagegen ein Problem, für das derzeit keine brauchbare Lösung existiert. In der Literatur beschriebene Migrationskonzepte und deren Schwachpunkte werden im folgenden vorgestellt.

3.5.3.1 Statusinformation in den Transportinstanzen

Bedingt durch den indirekten Transportansatz muß im Transportgateway für jede indirekte Transportverbindung zu einem mobilen System zusätzlich Statusinformation verwaltet werden. Es ist dies die Statusinformation der *F-Transportinstanz*, der Partnertransportinstanz des Festnetzrechners, und der *M-Transportinstanz*, der Partnertransportinstanz des mobilen Systems. Für jede der beiden genannten Transportinstanzen umfaßt die Statusinformation die im folgenden aufgelisteten Daten.

- Sendepuffer
  Der Sendepuffer enthält Nutzdaten, die bereits zur Partnertransportinstanz gesendet wurden, aber noch nicht bestätigt sind.

- Empfangspuffer
  Der Empfangspuffer enthält Nutzdaten, die korrekt empfangen wurden, aber noch nicht von der empfangenden Anwendung aus diesem entnommen wurden.

- Protokollkontrollblock
  Variablenwerte der jeweiligen Protokollinstanz, z.B. Timeoutwerte, geschätzte Paketumlaufzeiten, Bestätigungs-Sequenznummern und Sequenznummern bereits korrekt empfangener Nutzdaten gehören zum Protokollkontrollblock.

In Abb. 3.5 sind die zwei Transportinstanzen einer indirekten Transportverbindung in einem Transportgateway dargestellt. Die in den Transportinstanzen zu verwaltende Statusinformation ist in die Abbildung mit aufgenommen. Auf einem Zwischensystem, das als Transportgateway für eine indirekte Transportverbindung fungieren soll, muß diese Statusinformation verfügbar sein. Andernfalls kann das Zwischensystem für diese indirekte Verbindung nicht als Transportgateway operieren.

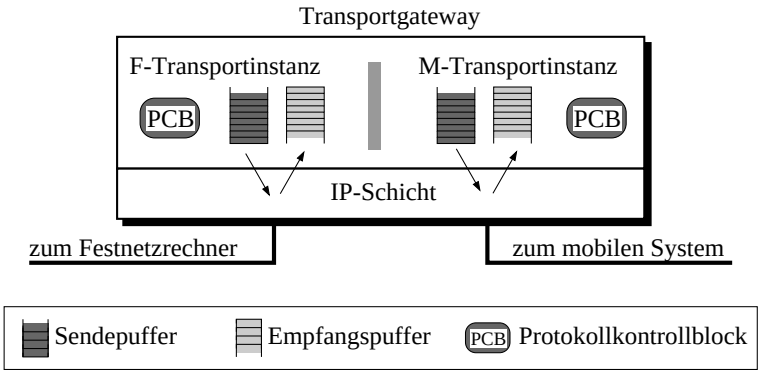


Abbildung 3.5: Statusinformation in den Transportinstanzen eines Transportgateways

Ändert sich die Route nach einem Subnetzwechsel des mobilen Systems dahingehend, daß die Pakete nicht mehr das zugehörige Transportgateway passieren, muß ein anderes in den neuen Datenpfad involviertes Zwischensystem die Funktion des Transportgateways übernehmen. Vom *alten Transportgateway*, das nicht mehr im Datenpfad liegt, muß die Statusinformation zu dem *neuen Transportgateway*, das im neuen Datenpfad lokalisiert ist, übertragen werden. Dies ist die Aufgabe der sogenannten *Migrationsunterstützung*. Als *aktives Transportgateway* wird das Transportgateway bezeichnet, auf dem die Transportinstanzen aktiv sind. Ein *passives Transportgateway* ist ein Transportgateway, auf das Statusinformation migriert wird, das aber noch nicht aktiviert wurde. Ein neues Transportgateway ist somit bis zu dem Zeitpunkt, zu dem die Statusinformation komplett verfügbar ist, ein passives Transportgateway, nach Aktivierung der Transportinstanzen wird es zum aktiven Transportgateway.

Werden Nutzdaten auch während der Migration zwischen dem Festnetzrechner und dem mobilen System übertragen, so hat dies fortlaufend Änderungen der zu migrierenden Statusinformation in der F-Transportinstanz und der M-Transportinstanz des Transportgateways zur Folge. Dies erschwert den Vorgang der Migration, der ein identisches Abbild der Statusinformation beim neuen Transportgateway verfügbar machen muß.

3.5.3.2 Existierende Migrationskonzepte

Von den in Kapitel 3.3.3 aufgeführten indirekten Transportansätzen beschäftigen sich lediglich [BB95a], [Bro97], [Wol99] und [WT98] mit dem Problem der Migration der Statusinformation. Diesen Ansätzen ist gemeinsam, daß unmittelbar nachdem das bisher als Gateway fungierende Zwischensystem nicht mehr im Datenpfad liegt, mit der Migration der Statusinformation begonnen wird.

Für die an der TU Berlin entwickelte Remote Socket Architecture wird von den Autoren vorgeschlagen, einen Multicast-basierten Ansatz für die Migration der Statusinformation zu verwenden [Wol99]. Wie dies im Detail realisiert werden soll, bleibt allerdings offen.

Für den M-TCP Ansatz wird in [Bro97] ein Verfahren zur Migration skizziert, bei dem die Protokollkontrollblöcke, jedoch keine Pufferinhalte vom alten zum neuen Transportgateway übertragen werden. Indem die Pakete von der Transportinstanz im Endsystem wiederholt werden, kann das neue Transportgateway die Pufferinhalte rekonstruieren. Nachdem die Protokollkontrollblöcke zum neuen Transportgateway migriert wurden, veranlaßt das neue Transportgateway die sendende Transportinstanz, die Pakete zu wiederholen und erfährt somit von den Pufferinhalten der Transportinstanzen. Eine Migration der Pufferinhalte vom alten zum neuen Transportgateway ist somit nicht erforderlich. In [Bro97] wird behauptet, mittels des beschriebenen Verfahrens die Pufferinhalte schneller auf dem neuen Transportgateway verfügbar machen zu können, als durch eine Übertragung der Puffer vom alten zum neuen Transportgateway. Es werden allerdings weder Messungen beschrieben noch Zahlen genannt, wie lange eine Migration dauert bzw. wie lange die Kommunikation in der Transportschicht unterbrochen ist.

Für den I-TCP Ansatz wird in [BB95a] ein Verfahren zur Migration der Statusinformation beschrieben. Da das Transportgateway bei diesem Ansatz auf einer Basisstation realisiert ist, muß nach jedem Basisstationswechsel auch das Transportgateway migriert werden. Die Transportinstanzen auf dem alten Transportgateway werden nach dem Basisstationswechsel des mobilen Systems deaktiviert und anschließend der Inhalt der Sendepuffer und der Empfangspuffer zuzüglich der Protokollkontrollblöcke der beiden Transportinstanzen zum Transportgateway auf der neuen Basisstation übertragen. Sobald die Statusinformation der Transportinstanzen beim neuen Transportgateway verfügbar ist, werden die Transportinstanzen aktiviert. Da die Transportinstanzen während der Migration deaktiviert (eingefroren) sind, wird das Verfahren als *Migration mit Einfrieren* bezeichnet. Von der Deaktivierung des alten Gateways bis zur Aktivierung des neuen Gateways ist, in Abhängigkeit von der Menge der zu migrierenden Statusinformation, bis zu 1.4 Sekunden keine Transportkommunikation möglich. Darüber hinaus sind die timerbasierte Übertragungswiederholung und die Lastkontrolle von TCP unter Umständen für eine über die Zeitdauer von 1.4 Sekunden hinausgehende Beeinträchtigung der Kommunikation verantwortlich.

Die durch die Migration der involvierten Transportinstanzen nach jedem Basisstationswechsel bedingten Unterbrechungen sind der wesentliche Nachteil der für I-TCP vorgestellten Migrationsunterstützung [BB95a]. Insbesondere bei picozellularen Netzen mit kleinen Zellen und häufigen Basisstationswechseln ist dieser Ansatz nicht praktikabel. Diese Migrationsunterstützung muß daher als nur bedingt einsetzbar eingestuft werden.

3.6 Zusammenfassung

In der Literatur sind eine Vielzahl von Lösungsansätzen beschrieben, um trotz Verbindungsunterbrechungen und Übertragungsfehlern – wie sie für die drahtlose Übertragung typisch sind – die Performance Einbußen von TCP zu verringern. Lokale Lösungen, die über dem drahtlosen Link oder zumindest in der Nähe des drahtlosen Links operieren, können in Grenzen durch geeignete Verfahren (z.B. Kodierung, Übertragungswiederholung) die höhere Fehleranfälligkeit des drahtlosen Links kompensieren, aber dennoch nicht vollständig vor den Endsystemen verbergen. Ein wesentlicher Vorteil der lokalen Lösungsansätze ist, daß sie – wie im Rahmen der vorliegenden Arbeit gefordert – keine Modifikation der TCP-Implementierung in den Festnetzrechnern notwendig machen. Allerdings kann nur ein Teil der lokalen Ansätze auch im Falle längerer Unterbrechungen des Übertragungskanals eine Reduktion des Slow-Start-Grenzwertes und des Lastkontrollfensters auf ihre Minimalwerte vermeiden. Abgesehen von den indirekten Transportansätzen sind bei allen lokal operierenden Lösungsansätzen deshalb Durchsatzeinbußen nach längeren Verbindungsunterbrechungen die Folge. Für die indirekten Transportansätze trifft dies nicht zu, da die TCP-Verbindung im Transportgateway terminiert wird und somit nicht über der drahtlosen Teilstrecke operiert. Aus den genannten Gründen erweist sich der indirekte Transportansatz, unter der Berücksichtigung der im Rahmen dieser Arbeit gestellten Anforderungen, als der Ansatz der Wahl.

Um den indirekten Transportansatz auch im Kontext mobiler Endsysteme einsetzen zu können, ist eine spezielle – über die globale Mobilitätsunterstützung auf Basis von Mobile IP hinausgehende – *Mobilitätsunterstützung für indirekte Transportansätze* erforderlich. Die für den I-TCP Ansatz entwickelte *Migration mit Einfrieren* [BB95a] bietet zwar eine Mobilitätsunterstützung für den indirekten Transportansatz, zeigt aber wegen der durch die Migration bedingten Unterbrechungen deutliche Schwächen. Ziel der eigenen Arbeiten ist es, eine optimierte Mobilitätsunterstützung für den indirekten Transportansatz zu entwickeln. Diese beinhaltet nicht nur ein Migrationskonzept, um die durch die Migration von Transportinstanzen bedingten Unterbrechungsdauern zu verkürzen, sondern zusätzlich ein Verfahren, um Migrationen unnötig zu machen bzw. zumindest die Zahl der erforderlichen Migrationen zu reduzieren. Diese Verfahren werden im folgenden Kapitel im Detail vorgestellt.

Kapitel 4

OMIT: Optimierte Mobilitätsunterstützung für indirekte Transportansätze

Ziel der in diesem Kapitel vorgestellten ***O**ptimierten **M**obilitätsunterstützung für **I**ndirekte **T**ransportansätze* (OMIT) ist es, die durch die Migration von Transportinstanzen bedingten Unterbrechungen der Kommunikation zu reduzieren. Diese Migrationen sind durch die Mobilität der Endsysteme bedingt. Zur Reduktion werden zwei Strategien eingesetzt. Zum einen wird versucht, die Anzahl der erforderlichen Migrationen zu verringern. Zum anderen wird zusätzlich ein Verfahren vorgeschlagen, das die durch eine Migration bedingte Unterbrechung der Transportkommunikation von den in [BB95a] genannten maximal 1.4 Sekunden auf konstant 0.01 Sekunden reduzieren kann. Das als *Fast Forwarding* bezeichnete Verfahren – eine Erweiterung für Mobile IP – und das Verfahren der *nebenläufigen Migration* wurden für diese Zwecke im Rahmen der vorliegenden Arbeit entwickelt.

In Kapitel 4.1 werden zunächst die Anforderungen behandelt, die für eine effiziente Mobilitätsunterstützung im Fall indirekter Ansätze erfüllt sein müssen. Es wird darauf eingegangen, welche dieser Anforderungen als erfüllt vorausgesetzt werden und welche der Anforderungen die im Rahmen der vorliegenden Arbeit entwickelten Verfahren adressieren. Das OMIT-Konzept, bestehend aus dem Fast-Forwarding-Verfahren zur Reduktion der Anzahl der notwendigen Migrationen und dem Verfahren der nebenläufigen Migration zur Verkürzung der Unterbrechungsdauer, wird in Kapitel 4.2 vorgestellt. Wie das OMIT-Konzept in die Architektur eines Transportgateways eingebettet wird, wird in Kapitel 4.3 diskutiert. Kapitel 4.4 behandelt im Detail die nebenläufige Migration, um die Statusinformation beim neuen Transportgateway verfügbar zu machen. Die Integration der entwickelten Konzepte in Mobile IP wird in Kapitel 4.5 vorgestellt. Eine Zusammenfassung folgt in Kapitel 4.6.

4.1 Anforderungen

Um den indirekten Transportansatz trotz der Mobilität eines Endsystems einsetzen zu können, können die im Rahmen dieser Arbeit entwickelten Mechanismen nicht für sich alleine betrachtet werden, sondern müssen im Zusammenhang mit den anderen in die Mobilitätsunterstützung involvierten Komponenten gesehen werden. Dies insbesondere deshalb, da nicht nur die

Migration der Transportinstanzen, sondern auch diese Komponenten für Unterbrechungen verantwortlich sein können. Zu berücksichtigen sind sowohl die Komponenten der lokalen als auch der globalen Mobilitätsunterstützung. Welche Anforderungen an die lokale bzw. globale Mobilitätsunterstützung und insbesondere an das OMIT-Konzept zu stellen sind, wird im folgenden ausgeführt.

4.1.1 Anforderungen an die lokale Mobilitätsunterstützung

Mittels Mechanismen der lokalen Mobilitätsunterstützung werden Basisstationswechsel der mobilen Systeme realisiert. Verschiedene Mobilkommunikationssysteme unterscheiden sich dahingehend, wie lange die durch Basisstationswechsel bedingten Unterbrechungen andauern und dahingehend, inwieweit Basisstationswechsel Paketverluste zur Folge haben. Einige Systeme leiten Pakete von einer Basisstation, bei der das mobile System vormals angemeldet war, die es aber inzwischen verlassen hat, an eine neue Basisstation weiter, bei der das mobile System derzeit angemeldet ist. Andere Systeme verwerfen hingegen solche Pakete und verlassen sich darauf, daß auf höheren Schichten des Protokollstacks die durch Paketverluste während eines Basisstationswechsels verursachten Übertragungsfehler durch Übertragungswiederholungen korrigiert werden.

Wie sich Basisstationswechsel effizient realisieren lassen ist nicht Gegenstand der Betrachtungen in der vorliegenden Arbeit. Hinsichtlich durch Basisstationswechsel bedingter Paketverluste werden keine Annahmen getroffen. Für die in der vorliegenden Arbeit entwickelten Konzepte ist es nicht relevant, ob Paketverluste während Basisstationswechseln vermieden werden können oder auftreten können. Wird der indirekte Transportansatz eingesetzt, ist es die Aufgabe des zwischen dem Transportgateway und dem mobilen System operierenden Transportprotokolls, durch Basisstationswechsel bedingte Paketverluste zu korrigieren.

Die Realisierbarkeit vom Basisstationswechseln mit nur kurzen Unterbrechungen wird im folgenden vorausgesetzt. Würde man von Basisstationswechsel mit signifikanten Unterbrechungen ausgehen, würde sich die Frage stellen, warum besonderes Augenmerk auf eine Migrationsunterstützung für den indirekten Transportansatz gelegt wird, die nur kurze Unterbrechungen der Kommunikation in der Transportschicht zur Folge hat. Daß die Annahme kurzer Unterbrechungen realistisch ist, zeigt das drahtlose lokale Netz WaveLAN [Wav97], das Basisstationswechsel innerhalb von ca. 20 ms abschließen kann.

4.1.2 Anforderungen an die globale Mobilitätsunterstützung

Wie bereits in Kapitel 2.1.5 beschrieben, ist es für die globale Mobilitätsunterstützung nicht ausreichend, Mechanismen für Basisstationswechsel in den Basisstationen und in den mobilen Systemen zu realisieren. Für die globale Mobilitätsunterstützung müssen in der Netzwerkschicht Verfahren bereitgestellt werden, um für mobile Systeme bestimmte Pakete zu dem aktuellen Aufenthaltsort zu routen.

Zusätzlich zu den im vorherigen Abschnitt beschriebenen, durch Basisstationswechsel bedingten Kommunikationsunterbrechungen ergibt sich durch die mobilitätsunterstützende Netzwerkschicht eine weitere Verzögerung, bis nach einem Subnetzwechsel die Kommunikation auf der Netzwerkschicht zwischen den Kommunikationspartnern wieder möglich ist. Ursachen für diese Unterbrechung sind:

- Erkennen eines Subnetzwechsel
  Erst nachdem das mobile System den Subnetzwechsel erkannt hat, kann es die Protokollverarbeitung der mobilitätsunterstützenden Netzwerkschicht veranlassen, das Routing dahingehend anzupassen, daß die für das mobile System bestimmten Pakete zum aktuellen Aufenthaltsort, d.h. in das aktuelle Subnetz, geroutet werden. Bei Mobile IP kann das Erkennen des Subnetzwechsels bis zu einer Sekunde dauern.

- Etablierung der Route in das neuen Subnetz
  Bis die in die Etablierung der neuen Route involvierten Instanzen durch die Protokollverarbeitung die neue Route etabliert haben, vergeht zusätzlich Zeit, die die Unterbrechungsdauer verlängert. Insbesondere Paketumlaufzeiten der Registrierungsanforderung bzw. der Registrierungsantwort zwischen dem Home Agent und dem mobilen System spielen hier eine Rolle. Im Fall einer großen Distanz zwischen dem Home Agent und dem mobilen System ist dies problematisch.

Um die im Rahmen der vorliegenden Arbeit entwickelten Mechanismen, die die durch die Migration von Transportinstanzen bedingten Unterbrechungsdauern deutlich reduzieren, gewinnbringend einsetzen zu können, dürfen sich auch durch die globale Mobilitätsunterstützung keine signifikanten Unterbrechungen der Kommunikation ergeben. Andernfalls würde sich auch hier die Frage stellen, warum bei der Migration der Transportinstanzen eine möglichst kurze Unterbrechung der Transportkommunikation angestrebt wird, obwohl die durch die globale Mobilitätsunterstützung bedingten Unterbrechungen signifikant sind.

Das sich im Internet für die Mobilitätsunterstützung zunehmend etablierende Protokoll Mobile IP kann kurze Unterbrechungen allerdings nicht gewährleisten. Bei Mobile IP vergeht bis zum Erkennen eines Subnetzwechsels bis zu eine Sekunde und bis zum Etablieren der neuen Route eine Zeitdauer, die in der Größenordnung der doppelten Paketlaufzeit zwischen dem Home Agent und dem mobilen System liegt. Der sinnvolle Einsatz von nur kurze Unterbrechungen bedingenden Strategien für die Migration der Transportinstanzen ist im Falle einer durch Mobile IP realisierten Mobilitätsunterstützung nicht möglich. Es sind Verfahren erforderlich, die die Unterbrechungsdauer der Kommunikation nach einem Subnetzwechsel verkürzen. Mittels Modifikationen an Mobile IP ist dies möglich.

Im Rahmen dieser Arbeit wurden zusätzlich zu den Migrationsstrategien für die zwei Transportprotokollinstanzen einer indirekten Transportverbindung zwei Verfahren für die Reduzierung der durch Mobile IP bedingten Unterbrechungsdauern entwickelt. Werden diese Verfahren in Mobile IP integriert, lassen sich die Unterbrechungsdauern nach Subnetzwechseln reduzieren und somit dann auch die Mechanismen für die Reduktion der durch die Migration von Transportinstanzen bedingten Unterbrechungszeiten gewinnbringend einsetzen. Das Fast-Forwarding-Konzept, das wie bereits beschrieben die Zahl der notwendigen Migrationen der Transportinstanzen verringern kann, ist auch einsetzbar, um die Unterbrechungsdauer nach einem Subnetzwechsel zu reduzieren. Als zweite Strategie wird eine schichtenübergreifende Kommunikation zwischen der Schicht 2 und Mobile IP realisiert, um Subnetzwechsel schneller erkennen zu können. Mobile IP wird von der Schicht 2 mittels eines Signals über jeden Basisstationswechsel informiert. Da es sich bei diesem Konzept nicht um ein Konzept zur Reduzierung der durch die Migration bedingten Unterbrechungen handelt, wird es nicht in diesem Kapitel behandelt. In Kapitel 5.1 wird auf das Konzept und seine Implementierung eingegangen.

4.1.3 Anforderungen an die Mobilitätsunterstützung für indirekte Ansätze

Die an die Mobilitätsunterstützung für indirekte Transportansätze zu stellenden Anforderungen können in zwei Klassen eingeteilt werden. Zum einen in solche Anforderungen, die auf jeden Fall erfüllt sein müssen, um überhaupt den indirekten Transportansatz auch für mobile Systeme einsetzen zu können. Zum anderen in solche, die an eine optimierte Mobilitätsunterstützung zu stellen sind und die von dem OMIT-Konzept erfüllt werden. Beide Klassen werden im folgenden betrachtet.

4.1.3.1 Grundsätzliche Anforderung: Transportgateway im Datenpfad

Ein grundlegendes Problem der indirekten Transportansätze ist, daß das Transportgateway immer im Datenpfad zwischen dem Festnetzrechner und dem mobilen System liegen muß. Auf Grund der sich durch die Mobilität eines mobilen Systems ergebenden Routenänderungen wird das Transportgateway ggf. abgekoppelt. Die folgenden zwei Verfahren ermöglichen es, trotz der Ortswechsel eines mobilen Systems den indirekten Transportansatz einzusetzen:

- Migration der Transportinstanzen auf ein anderes Transportgateway oder
- Erzwingen des Routings über das andernfalls abgekoppelte Transportgateway.

Migration der Transportinstanzen
In Abb. 4.1a ist eine Migration der Transportinstanzen auf ein anderes Transportgateway dargestellt. Nach dem Ortswechsel des mobilen Systems werden an das mobile System adressierte bzw. von ihm abgesendete Pakete über das Zwischensystem geroutet, in dem das Transportgateway II realisiert ist. Die Transportkommunikation kann erst dann wieder aufgenommen werden, sobald die Statusinformation von Transportgateway I bei Transportgateway II verfügbar ist und somit Transportgateway II die Kopplung der beiden Transportverbindungen übernehmen kann.

Die Migration der Statusinformation wird sofort nach dem Ortswechsel erforderlich, da das alte Transportgateway nicht mehr im Datenpfad liegt. Dies gilt auch für die in Kapitel 3.5.3.2 beschriebene Migration mit Einfrieren, die beim I-TCP Ansatz angewandt wird. Da bei dem I-TCP Ansatz das Transportgateway auf einer Basisstation realisiert wird, muß bei jedem Basisstationswechsel migriert werden. Als Folge ergibt sich bei jedem Basisstationswechsel eine Unterbrechung von bis zu 1.4 Sekunden.

Auf Grund der nach der Migration kürzeren Entfernung zwischen dem als Transportgateway fungierenden Zwischensystem und dem mobilen System lassen sich von dem über dieser Teilstrecke operierenden Transportprotokoll Übertragungsfehler schneller korrigieren. Der im folgenden beschriebene Ansatz, der das Routing über das alte Transportgateway erzwingt, hat eine größere Distanz zwischen Transportgateway und mobilem System und somit eine langsamere Korrektur von Übertragungsfehlern zur Folge.

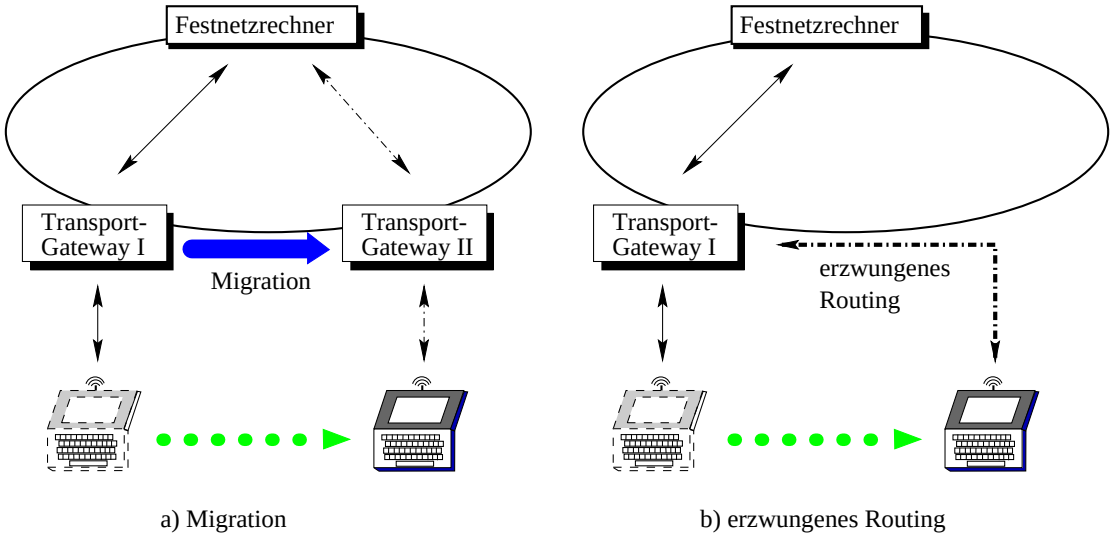


Abbildung 4.1: Migration vs. erzwungenes Routing

Erzwingen des Routings
Anstatt nach Ortswechseln eine Migration der Transportinstanzen vorzunehmen, wird das Routing dahingehend geändert, daß das bisherige Transportgateway weiterhin im Datenpfad liegt. Da keine Migration der Transportinstanzen vorgenommen wird, können die durch die Migration bedingten Unterbrechungen der Kommunikation auf der Transportebene vermieden werden. In Abb. 4.1b ist skizziert, wie nach einem Ortswechsel eines mobilen Systems an das mobile System adressierte bzw. vom ihm gesendete Pakete weiterhin über das Transportgateway I geroutet werden und somit keine Migration vom Transportgateway I auf ein anderes Transportgateway notwendig ist. Mittels des in der vorliegenden Arbeit entwickelten Fast-Forwarding-Konzeptes kann das Routing über das alte Transportgateway erzwungen werden. Eine Gegenüberstellung der Vorteile und Nachteile der in Abb. 4.1 dargestellten Ansätze zeigt Tabelle 4.1.

Migration der Instanzen	Erzwungenes Routing
– Subnetzwechsel bedingt Migration	+ keine Migration der Transportinstanzen notwendig
– Transportkommunikation für 1.4 Sekunden wegen der Migration unterbrochen [BB95a]	– ggf. ineffizientes Routing
+ geringe Distanz zwischen Transportgateway und mobilem System	– wachsende Distanz zwischen dem Transportgateway und dem mobilem System

Tabelle 4.1: Migration vs. erzwungenes Routing

Keiner der beiden Ansätze ist für sich alleine betrachtet als Lösung geeignet, um den indirekten Transportansatz auch im Falle häufiger Ortswechsel mobiler Systeme einzusetzen. Im Zusammenspiel läßt sich aber einerseits durch das erzwungene Routing eine zu häufige Migration der Transportinstanzen vermeiden, anderseits aber – im Falle einer zu großen Distanz

zwischen dem Transportgateway und dem mobilen System – durch eine Migration der Transportinstanzen diese Distanz reduzieren. Die Strategie, beide Ansätze zusammen einzusetzen, wird bei dem OMIT-Konzept verfolgt und umgesetzt.

4.1.3.2 Anforderungen an eine optimierte Mobilitätsunterstützung

Um eine optimierte Mobilitätsunterstützung für indirekte Transportansätze zu erreichen, wurden die im folgenden aufgelisteten Anforderungen an das im Rahmen der vorliegenden Arbeit entwickelte Konzept gestellt:

- seltenere Notwendigkeit einer Migration,
- kürzere Unterbrechungen im Falle einer Migration und
- Integration mit Mobile IP.

Ist eine Migration seltener erforderlich und läßt sich im Falle einer Migration diese mit kürzeren Unterbrechungsdauern realisieren, so können insgesamt die durch die Mobilität eines Endsystems bedingten Kommunikationsunterbrechungen reduziert werden. Mittels des *Fast Forwardings* läßt sich die Anzahl der notwendigen Migrationen verringern und weiterhin der *Zeitpunkt der Migration* von dem Zeitpunkt entkoppeln, zu dem der Subnetzwechsel erfolgt. Kürzere Unterbrechungen werden mittels des Konzeptes der *nebenläufigen Migration* erreicht, das zeitgleich zur Migration die Fortsetzung der Kommunikation in der Transportschicht zuläßt. Die Transportinstanzen werden während der Migration nur sehr kurz (ca. 10 ms) deaktiviert. Die Integration mit Mobile IP ist als wesentlich zu erachten, da sich Mobile IP zunehmend als Protokoll der Wahl für die globale Mobilitätsunterstützung IP-basierter Endsysteme herauskristallisiert. In Tabelle 4.2 ist die in dieser Arbeit realisierte optimierte Mobilitätsunterstützung für indirekte Transportansätze der für I-TCP vorgeschlagenen gegenübergestellt.

	Mobilitätsunterstützung in I-TCP	Mobilitätsunterstützung durch OMIT	
		Zielsetzung	Mechanismus
Migrationszeitpunkt	nach jedem Wechsel der Basisstation	Zeitpunkt frei wählbar	Mobile IP zzgl. Fast Forwarding (Kap. 4.2.2)
Migrationsstrategie	Unterbrechung der TP-Kommunikation während der Migration	TP-Kommunikation während der Migration möglich	nebenläufige Migration & gezielte Pufferauswahl (Kap. 4.2.3)

Tabelle 4.2: Gegenüberstellung der Migrationskonzepte

Die Verfahren, um die in der Tabelle aufgeführten Zielsetzungen des eigenen Ansatzes für eine optimierten Mobilitätsunterstützung für indirekte Ansätze umzusetzen, werden im nachfolgenden Kapitel vorgestellt.

4.2 Das OMIT-Konzept

Zur Reduzierung der durch Migrationen bedingten Unterbrechungen sind zwei Strategien anwendbar. Zum einen können Mechanismen und Strategien eingesetzt werden, die die Zahl der notwendigen Migrationen reduzieren. Dies ist durch geschickte Positionierung eines Transportgateways, die in Kapitel 4.2.1 beschrieben wird, und durch die in Kapitel 4.2.2 vorgestellte Fast-Forwarding-Erweiterung für Mobile IP möglich. Zum anderen kann, falls tatsächlich eine Migration vorgenommen werden muß, durch spezielle Verfahren die Unterbrechungszeit reduziert werden. Das in Kapitel 4.2.3 beschriebene Konzept der nebenläufigen Migration ist hierfür geeignet.

Die Betrachtungen in diesem Unterkapitel abstrahieren von konkreten Realisierungen der Mobilitätsunterstützung in der Netzwerkschicht. Der Fokus liegt auf den konzeptionellen Betrachtungen. Wie sich die entwickelten Ideen in das sich zunehmend für die Mobilitätsunterstützung etablierende Protokoll Mobile IP integrieren lassen, wird erst in Kapitel 4.5 erläutert.

4.2.1 Positionierung des Transportgateways

Hinsichtlich der Strategie, auf welchem System das Transportgateway realisiert wird, sind verschiedene Ansätze möglich. Damit der indirekte Transportansatz effizient operieren kann, sind kurze Paketumlaufzeiten zwischen dem Transportgateway und dem mobilen System erforderlich. Längere Paketumlaufzeiten hätten eine langsamere Fehlerkorrektur zwischen diesen Systemen zur Folge.

Das Transportgateway kann an dem Übergang zwischen dem drahtgebundenen und dem drahtlosen Teil des Netzwerkes, d.h. auf einer Basisstation, plaziert werden. Alternativ dazu ist es auch vorstellbar, das Transportgateway auf einem Rechner des Subnetzes, in dem sich das mobile System aktuell befindet, zu realisieren. In diesem Falle kann das Transportgateway entweder auf einem Router oder auf einem ausgewiesenen Rechner des Subnetzes implementiert werden. Eine dritte sich bietende Alternative wäre es, das Transportgateway auf einem Rechner eines anderen Subnetzes zu installieren. Kriterien, die für die Entscheidung, auf welchem System das Transportgateway realisiert wird, berücksichtigt werden müssen, sind die folgenden:

- Häufigkeit der Migration der Statusinformation
  Transportinstanzen von Transportverbindungen auf Transportgateways, die nahe am aktuellen Aufenthaltsort eines mobilen Systems realisiert sind, müssen häufiger migriert werden, als solche die weiter innerhalb des Netzwerkes angesiedelt sind. Ursache hierfür ist eine höhere Wahrscheinlichkeit, daß nach einem Subnetzwechsels das Transportgateway nicht mehr im Datenpfad liegt und somit eine Migration notwendig wird.

- Skalierbarkeit
  Wird ein Transportgateway nicht am Rand des Netzwerkes, sondern weiter innerhalb des Netzwerkes realisiert, so ergibt sich als unmittelbare Folge daraus, daß dieses Transportgateway für viele Transportverbindungen verschiedener mobiler Systeme als Gateway fungiert. In der Literatur beschriebene Untersuchungen, auf die bereits in Kapitel 3.5.2 eingegangen wurde, zeigen, daß die Anzahl der in einem Zwischensystem

unterstützbaren indirekten Transportverbindungen in der Größenordnung weniger hundert Transportverbindungen liegt. Transportgateways können aus diesem Grunde nicht auf zentralen Netzwerkknoten, über die Tausende von Verbindungen geroutet werden, realisiert werden.

4.2.1.1 Stand der Forschung: Transportgateway auf der Basisstation

In [BB95b] wird der Ansatz verfolgt, das Transportgateway am Übergang vom drahtgebundenen Teil des Netzwerkes in den drahtlosen Teil zu realisieren. In dieser Arbeit kommt keine käuflich erhältliche Basisstation zum Einsatz. Stattdessen wird in einen Unix-basierten PC mittels einer WaveLAN PCMCIA Einsteckkarte ein zusätzliches Interface integriert, über das die drahtlose Kommunikation abgewickelt wird.

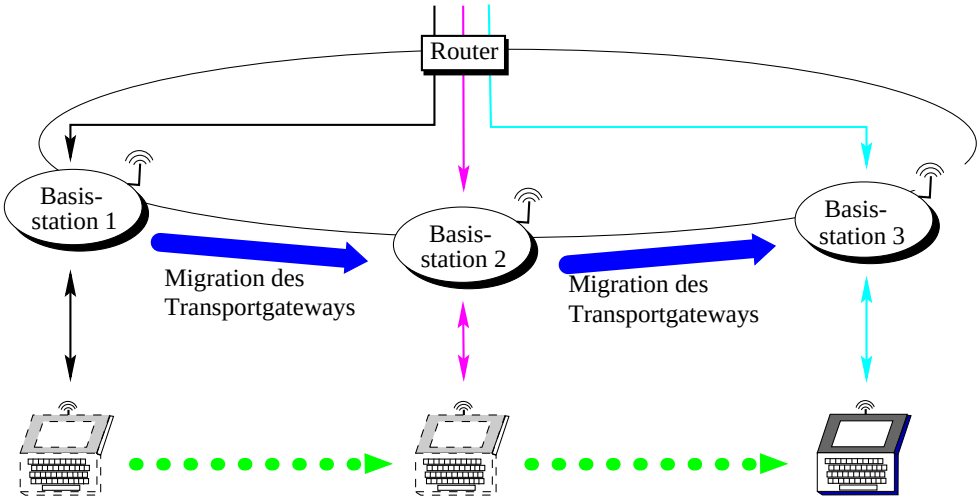


Abbildung 4.2: Transportgateway auf der Basisstation

Abb. 4.2 zeigt ein Szenario, bei dem das Transportgateway auf einer Basisstation realisiert ist. Durchgezogene Linien mit Doppelpfeil repräsentieren die Transportverbindung zwischen dem mobilen System und dem Transportgateway, durchgezogene Linien mit einem einzelnen Pfeil die Transportverbindung zwischen Transportgateway und einem Festnetzrechner. Das mobile System ist zunächst über die Basisstation 1 an das Subnetz angebunden. Auf Basisstation 1 ist auch das Transportgateway realisiert, das die Kopplung der indirekten Transportverbindungen des mobilen Systems übernimmt. Ändert das mobile System seinen Aufenthaltsort und wird es über die Basisstation 2 an das Subnetz angebunden, werden die Pakete nicht mehr über Basisstation 1 sondern über Basisstation 2 geroutet. Als unmittelbare Folge davon können die Transportverbindungen des mobilen Systems auch nicht mehr in Basisstation 1 gekoppelt werden. Stattdessen muß das Transportgateway auf Basisstation 2 migriert werden und dort die Kopplung der Transportverbindungen erfolgen. Analog ist bei einem weiteren Wechsel des mobilen Systems zu der Basisstation 3 zu verfahren.

Der wesentliche Nachteil dieses Ansatzes ist darin zu sehen, daß auch nach Basisstationswechseln, bei denen das mobile System zwar die Basisstation aber nicht das Subnetz gewechselt hat, das Transportgateway migriert werden muß.

Insbesondere im Fall mikrozellularer oder gar pikozellularer Netze ist dieser Ansatz wegen der häufigen Basisstationswechsel und der dann häufig notwendigen Migrationen proble-

matisch. Er skaliert für häufige Wechsel nicht. Oszillierende Wechsel sind bei diesem Ansatz ebenfalls problematisch. Darüber hinaus ist es das Ziel der Hersteller, Basisstationen möglichst einfach und billig zu realisieren. Dies spricht ebenfalls dagegen, zusätzlich die Funktionalität eines Transportgateways in Basisstationen zu integrieren.

4.2.1.2 Transportgateway auf Rechner des gleichen Subnetzes

Anstatt das Transportgateway auf der Basisstation zu realisieren, kann es auch auf einem System innerhalb des gleichen Subnetzes plaziert werden. Prinzipiell gibt es dazu zwei Möglichkeiten:

- Auf einem Router, der das Subnetz an das Internet anbindet, oder
- auf einem ausgewiesenen System des Subnetzes.

Beiden Ansätzen ist gemeinsam, daß im Falle eines Basisstationswechsels eines mobilen Systems die Transportinstanzen nur dann migriert werden müssen, falls der Basisstationswechsel auch einen Wechsel des Subnetzes zur Folge hat. Da ein Basisstationswechsel also nicht unbedingt eine Migration des Transportgateways impliziert, kann im Vergleich zu der Realisierungsvariante, bei der das Transportgateway auf der Basisstation implementiert wird, die Anzahl der notwendigen Migrationen reduziert werden. Die Realisierung eines Transportgateways auf einem Router ist in Abb. 4.3 dargestellt, die sich ergebende Situation im Falle der Realisierung des Transportgateways auf einem ausgewiesenen System zeigt Abb. 4.4.

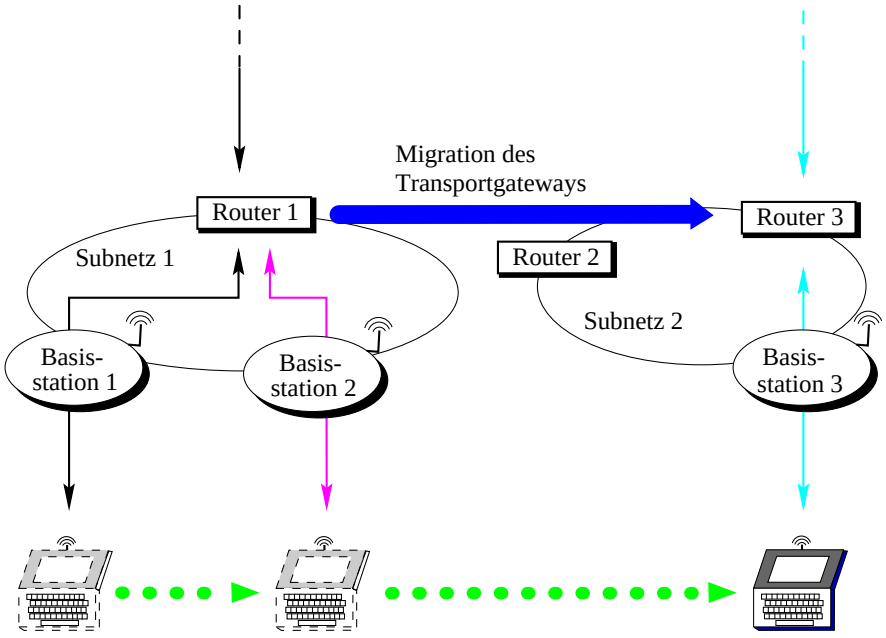


Abbildung 4.3: Transportgateway auf einem Router

Das mobile System meldet sich nacheinander bei Basisstation 1, Basisstation 2 bzw. Basisstation 3 an. Da der Wechsel von Basisstation 1 zu Basisstation 2 nicht zugleich auch einen Subnetzwechsel zur Folge hat, muß in diesem Falle das Transportgateway nicht migriert werden, sondern kann auf Router 1 verbleiben. Der Wechsel von Basisstation 2 zu Basisstation 3

zieht hingegen einen Wechsel von Subnetz 1 in das Subnetz 2 nach sich. An das mobile Systems adressierte Pakete werden somit nicht mehr unbedingt über Router 1 geroutet. Das Transportgateway ist in diesem Falle abgekoppelt. Aus diesem Grunde müssen die Transportinstanzen auf Router 3 migriert werden.

Da das Subnetz 1 durch genau einen Router an das Internet angebunden ist, ist bereits durch die Topologie sichergestellt, daß alle IP-Pakete über den Router 1 und das dort implementierte Transportgateway geroutet werden. Spezielle Mechanismen, die für das Routing über das Transportgateway sorgen, sind somit nicht erforderlich. Erfolgt hingegen – wie bei Subnetz 2 – die Anbindung über mehr als einen Router, ist es prinzipiell möglich, daß die Pakete über den Router, der nicht als Transportgateway fungiert, in das Subnetz geleitet werden. Im Falle mehrerer Router sind also spezielle Routingmechanismen notwendig, die das Routing über das Transportgateway erzwingen.

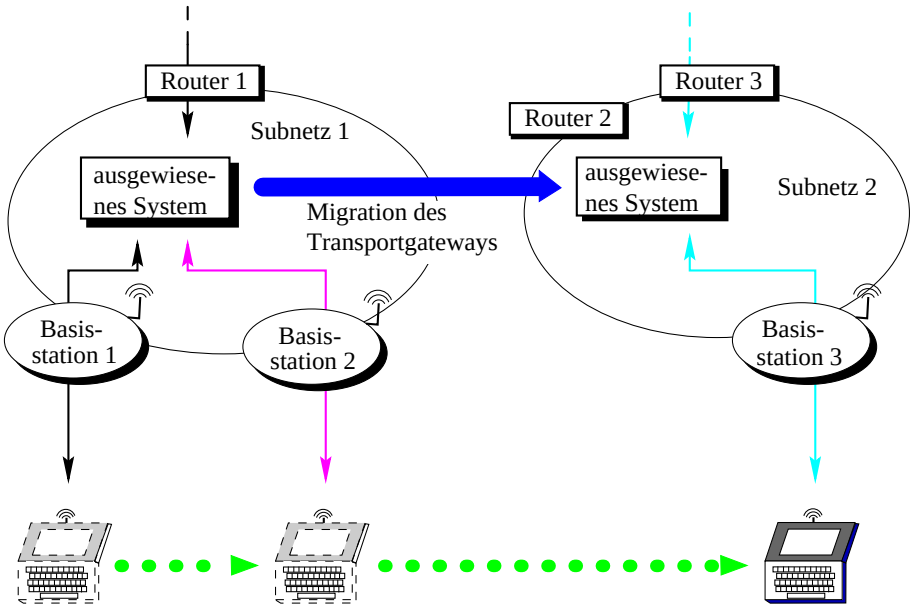


Abbildung 4.4: Transportgateway auf ausgewiesenem System

In Abb. 4.4 ist die Situation dargestellt, falls das Transportgateway im gleichen Subnetz auf einem ausgewiesenen System realisiert wird. Wie auch im Falle der Realisierung des Transportgateways auf einem Router hat der Wechsel von Basisstation 1 zu Basisstation 2 keinen Subnetzwechsel zur Folge. Somit ist auch eine Migration des Transportgateways nicht erforderlich. Der Wechsel zu Basisstation 3 hingegen macht die Migration des Transportgateways notwendig. Hinsichtlich der Häufigkeit der Migration ist es irrelevant, ob das Transportgateway auf einem Router oder einem ausgewiesenen System im Subnetz realisiert wird.

Spezielle Routingmechanismen sind dagegen bei der in Abb. 4.4 skizzierten Variante generell erforderlich, da andernfalls nicht garantiert werden kann, daß die Pakete über das auf dem ausgewiesenen System realisierte Transportgateway geroutet werden. Da wie in Kapitel 2.1.5 beschrieben für die globale Mobilitätsunterstützung in der Netzwerkschicht ohnehin spezielle Routingmechanismen erforderlich sind, ist dies nicht als Nachteil zu werten.

Wird das Transportgateway auf einem ausgewiesenen System plaziert, so müssen für das mobile System bestimmte Pakete zweimal im Subnetz über das lokale Netzwerk übertragen werden. Die doppelte Übertragung der Pakete über das lokale drahtgebundene Netzwerk ist

aber nur dann als signifikanter Nachteil zu werten, falls für die übertragenen Datenmengen ein erheblicher Anteil der im Subnetz verfügbaren Bandbreite erforderlich ist. Die doppelte Übertragung ist nicht problematisch, falls im Bereich der drahtgebundenen Übertragung wesentlich größere Bandbreiten als bei der drahtlosen Übertragung zur Verfügung stehen.

4.2.1.3 Transportgateway auf Rechner eines anderen Subnetzes

Alternativ zu den beiden vorgestellten Varianten kann das Transportgateway auch auf einem Rechner, der weiter innerhalb des Netzwerkes angesiedelt ist, plaziert werden. Abb. 4.5 zeigt ein derartiges Szenario. Sowohl im Falle von Basisstationswechseln innerhalb eines Subnetzes als auch falls das mobile System zwischen den dargestellten Subnetzen 1...3 wechselt, ist keine Migration des auf dem Router 6 realisierten Transportgateways notwendig. Ein Wechsel zu Basisstation 4 erfordert im dargestellten Szenario dagegen wieder eine Migration des Transportgateways.

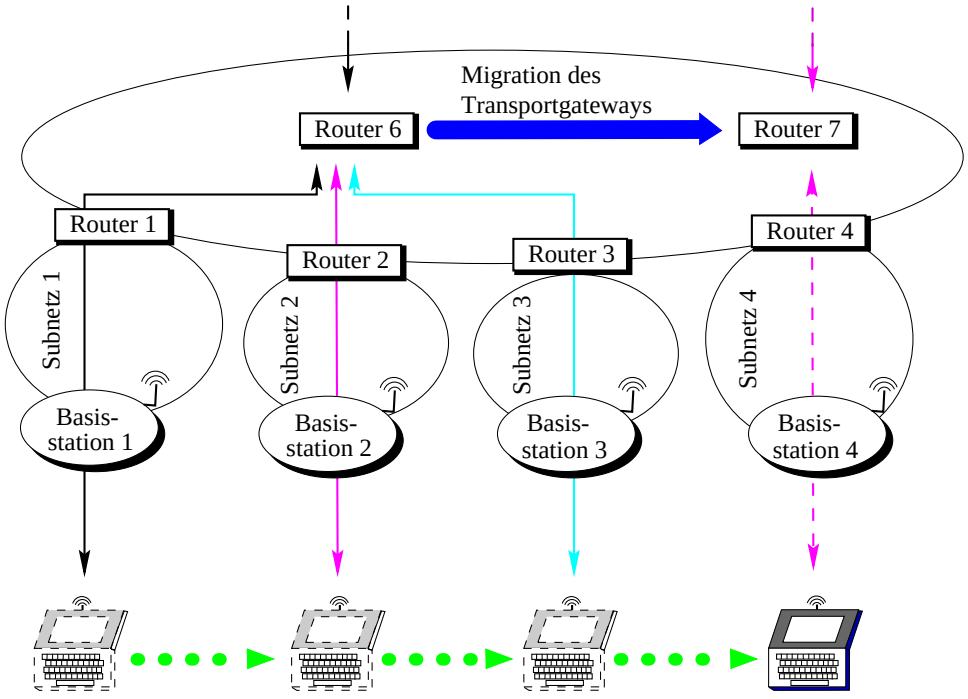


Abbildung 4.5: Transportgateway in einem anderen Subnetz

Hinsichtlich der Anzahl der notwendigen Migrationen ist diese Variante im Vergleich zu den beiden bereits beschriebenen Strategien als besser geeignet zu bewerten. Allerdings ist ihr Einsatz unter dem Aspekt der Skalierbarkeit problematisch. Da der Router 6 für alle mobilen Systeme, die über eines des Subnetze 1...3 an das Festnetz angebunden sind, als Transportgateway fungieren muß, sind unter Umständen für die Transportprotokollverarbeitung auf diesem System nicht ausreichend Ressourcen verfügbar. Je weiter innerhalb des Netzwerkes ein Transportgateway realisiert wird, um so problematischer ist der Aspekt der Skalierbarkeit. Die Wahl des Zwischensystems, das als Transportgateway für ein bestimmtes mobiles Endsystem fungieren soll, kann optimiert werden, falls der Grad der Mobilität des Endsystems mit berücksichtigt wird. Für mobile Endsysteme, die selten das Subnetz wechseln, bietet es sich an, das Transportgateway ganz am Rand des Netzwerkes zu plazieren. Für hochgradig

mobile Endsysteme, die häufig zwischen verschiedenen Subnetzen wechseln, ist es sinnvoll, das Transportgateway weiter innerhalb des Netzwerkes zu realisieren.

4.2.1.4 Bewertung der Positionierungsvarianten

Tabelle 4.3 faßt die verschieden Positionierungsvarianten mit ihren jeweiligen Vor- und Nachteilen zusammen. Inwieweit einzelne Kriterien bei den verschieden Varianten erfüllt werden, wird durch die folgenden Bewertungszeichen zum Ausdruck gebracht: ++ sehr gut, +/− akzeptabel, − schlecht, −− sehr schlecht.

	Gateway auf der Basisstation	Gateway auf Router im gleichen Subnetz	Gateway auf ausgewiesenem System im gl. Subnetz	Gateway auf Router in anderem Subnetz
Häufigkeit der Migration	−−	+/−	+/−	++
Skalierbarkeit	++	+/−	+/−	−−
Routinganforderungen	++	+/−	−−	−

Tabelle 4.3: Positionierung des Transportgateways

Der Ansatz, das Transportgateway auf einer Basisstation zu realisieren, kommt im Rahmen der vorliegenden Arbeit nicht in Frage, da als unmittelbare Folge dieser Strategie bei jedem Basisstationswechsel eine Migration der involvierten Transportinstanzen notwendig wäre. Aufgrund unzureichender Skalierbarkeit scheidet auch der Ansatz aus, das Transportgateway weiter innerhalb des Netzwerkes in einem anderen Subnetz zu plazieren. Als Alternativen bleiben somit nur das Transportgateway auf dem Router des gleichen Subnetzes oder auf einem ausgewiesenen System des gleichen Subnetzes zu realisieren.

Wie bereits diskutiert, sind für eine globale Mobilitätsunterstützung spezielle Routingmechanismen erforderlich. Insofern ist es nicht als Nachteil zu werten, daß der Ansatz, der das Transportgateway auf einem ausgewiesenen System realisiert, spezielle Routingmechanismen erfordert, während sie im Fall eines auf dem Router implementierten Transportgateways nicht notwendig sind.

Ein Konzept, das das Transportgateway auf einem Router implementiert, ist nicht unbedingt dazu geeignet, das Transportgateway alternativ auch auf einem ausgewiesenen System zu realisieren, da nicht sichergestellt ist, daß die Pakete über das ausgewiesene System geroutet werden. Umgekehrt kann ein Konzept, das für das Routing der Pakete über ein als Transportgateway operierendes, ausgewiesenes System sorgt, auch eingesetzt werden, um zu erzwingen, daß die Pakete über den Router transportiert werden. Dieser Router kann somit die Funktion eines Transportgateways übernehmen. Da das Konzept, das Transportgateway auf einem ausgewiesenen System zu realisieren, die größere Flexibilität bietet, wird es im Rahmen der vorliegenden Arbeit verfolgt.

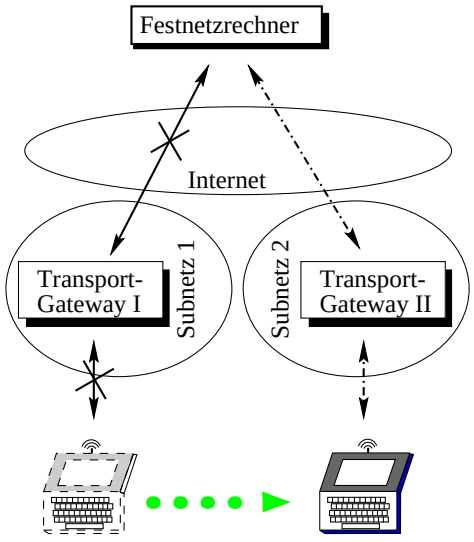
4.2.2 Vermeidung der Migration durch Fast Forwarding

Im vorangegangen Abschnitt wurde diskutiert, inwieweit durch eine geschickte Wahl des Transportgateways erreicht werden kann, daß auch nach einem Subnetzwechsel die Pakete

des mobilen Systems über das Transportgateway geroutet werden, ohne in das Routing einzugreifen. Die Idee des im folgenden *Fast Forwarding* genannten Ansatzes hingegen ist es, gezielt in das Routing einzugreifen und somit das Routing über das aktuell als Transportgateway operierende System zu erzwingen. Das Fast-Forwarding-Konzept erlaubt es, das alte Transportgateway auch dann noch als Transportgateway für indirekte Transportverbindungen zu nutzen, falls das mobile System inzwischen in ein anderes Subnetz gewechselt ist. Somit ergibt sich aus einem Subnetzwechsel nicht zwangsläufig die Notwendigkeit, unmittelbar nach dem Subnetzwechsel auch das Transportgateway auf ein anderes Zwischensystem zu migrieren. Die Fast-Forwarding-Strategie bietet die folgenden Vorteile:

- Entkopplung des Subnetzwechsels und des Migrationszeitpunktes und
- seltenere Migration der Transportinstanzen.

Um den Vorteil des Fast Forwardings zu verdeutlichen, wird einem Szenario ohne Fast Forwarding ein Szenario mit Fast Forwarding gegenübergestellt. Abb. 4.6a zeigt die Situation, falls das Fast Forwarding nicht zum Einsatz kommt. Der zugehörige Pseudocode ist in Abb. 4.6b dargestellt. Sobald das mobile System in das Subnetz 2 gewechselt ist, veranlaßt die globale Mobilitätsunterstützung in der Netzwerkschicht, daß an das mobile System adressierte Pakete direkt in das Subnetz 2 geroutet werden. Da die Pakete somit nicht mehr das Transportgateway 1 passieren, wird dieses deaktiviert. Bevor das Transportgateway 2 als aktives Transportgateway fungieren kann, muß die Statusinformation zu Transportgateway 2 migriert werden. Erst nach Abschluß der Migration ist die Kommunikation auf der Transportebene über das Transportgateway 2 wieder möglich. Als wesentlicher Nachteil dieses Verfahrens ist zu werten, daß unmittelbar nach einem Subnetzwechsel die Migration des Transportgateways zwingend notwendig wird. Die durch die Migration bedingte Unterbrechung der Transportkommunikation kann somit nicht vermieden werden.



a)

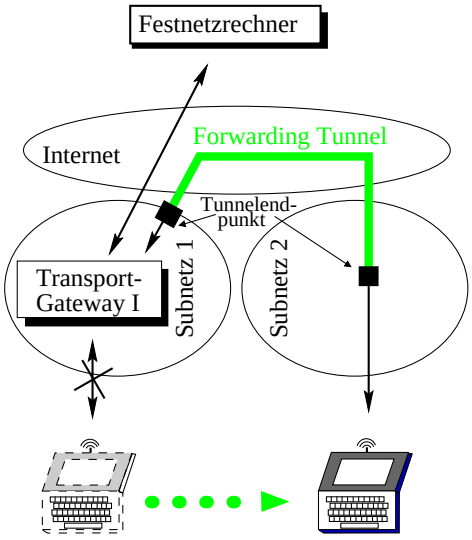
```
if (SubnetzWechsel)  {
  deaktiviere_altesTG();
  /* direkte Route ins neue */
  /* Subnetz: altes TG      */
  /* abgekoppelt            */
  etabliere_neueRoute();

  migriere_TPinstanzen();
  aktiviere_neuesTG();
  aufnahme_TPkommunikation();
}
```

b)

Abbildung 4.6: Routing ohne Fast Forwarding und zugehöriger Pseudocode

Wird das Fast-Forwarding-Konzept angewandt, so ergibt sich die in Abb. 4.7a dargestellte Situation. Nachdem das mobile System in das Subnetz 2 gewechselt ist, wird nicht die Etablierung einer neuen Route vom Festnetzrechner in das Subnetz 2 veranlaßt, sondern stattdessen

ein sogenannter Forwarding Tunnel von Subnetz 1 in das Subnetz 2 eingerichtet. Über die Forwarding Route werden sowohl für das mobile System bestimmte Pakete als auch vom mobilen System gesendete Pakete transportiert. In der Praxis läßt sich diese Forwarding Route durch einen bidirektionalen Tunnel realisieren. Sobald die Forwarding Route eingerichtet ist, kann das Transportgateway 1 im Subnetz 1 wieder als Transportgateway fungieren. Ein Subnetzwechsel erfordert somit nicht notwendigerweise eine Migration der Transportinstanzen. Damit ergeben sich insgesamt weniger Migrationen und die durch eine Migration bedingten negativen Auswirkungen auf die Transportkommunikation werden geringer. Eine Migration des Transportgateways 1 auf ein Transportgateway im Subnetz 2 zu einem späteren Zeitpunkt wird durch dieses Verfahren aber nicht ausgeschlossen.




```
if (SubnetzWechsel) {
  /* Forwarding vom alten ins */
  /* neue Subnetz: altes TG   */
  /* nicht abgekoppelt        */
  etabliere_ForwardingRoute();
  aufnahme_TPkommunikation();
}
```

b)

Abbildung 4.7: Routing mit Fast Forwarding und zugehöriger Pseudocode

Durch den Einsatz des Fast-Forwarding-Konzeptes wird der Zeitpunkt der Migration vom Zeitpunkt des Subnetzwechsels entkoppelt. Somit bietet sich die Möglichkeit, eventuell ganz auf die Migration zu verzichten und die aktiven Transportinstanzen weiterhin auf dem alten Transportgateway zu belassen. Bei der Entscheidung, ob das Transportgateway in Subnetz 1 verbleibt, muß berücksichtigt werden, inwieweit sich durch das Forwarding zusätzlich eine signifikante Verzögerung ergibt. Wird die Verzögerung zwischen dem aktiven Transportgateway und dem mobilen System zu groß, so geht der Vorteil einer schnellen und effizienten Fehlerkorrektur auf der Transportebene zwischen dem Transportgateway und dem mobilen System verloren. Welche zusätzlichen Verzögerungen noch toleriebar sind, hängt von dem zwischen dem Transportgateway und dem mobilen System verwendeten Transportprotokoll ab. Darüber hinaus ist auf die Migration zu verzichten, falls aus Sicht des mobilen Systems ein Wechsel zurück in das vorherige Subnetz absehbar ist. Oszillierende Wechsel haben somit nicht jedesmal die Migration der Transportinstanzen zur Folge.

Sollen die aktiven Transportinstanzen auf ein anderes System migriert werden, bietet die Entkopplung des Migrationszeitpunktes und des Zeitpunktes des Subnetzwechsel die Möglichkeit, für die Migration einen günstigen Zeitpunkt zu wählen und bis zum Zeitpunkt der Migration weiterhin die Kommunikation in der Transportschicht zu ermöglichen. Als günstig ist ein Migrationszeitpunkt anzusehen, zu dem lediglich eine geringe Menge an Statusinfor-

mation zum neuen Transportgateway zu migrieren ist. Dies ist der Fall, falls die Anzahl bestehender Verbindungen des mobilen Systems gering ist bzw. die Verbindungen temporär nicht aktiv sind, d.h. die zu migrierenden Puffer nicht gefüllt sind.

Das im nächsten Abschnitt vorgestellte Konzept der nebenläufigen Migration setzt die Realisierung des Fast-Forwarding-Konzeptes voraus. Da trotz eines Subnetzwechsels keine Migration erforderlich ist, kann die Kommunikation auf der Transportebene weiterhin aktiv sein. Sie ist sogar während der Migration der Pufferinhalte zum neuen Transportgateway aktiv. Die durch die Migration bedingten Unterbrechungszeiten lassen sich somit reduzieren.

4.2.3 Nebenläufige Migration der Statusinformation

Das Fast-Forwarding-Konzept und die geschickte Positionierung des Transportgateways reduzieren zwar die Zahl der notwendigen Migrationen der Transportinstanzen, im Falle einer Migration ergeben sich aber trotzdem Unterbrechungen der Transportkommunikation. Wesentlicher Nachteil des in [BB95a] für die Migration vorgeschlagenen Verfahrens ist die durch die Migration bedingte Unterbrechung der Transportkommunikation für eine Dauer von bis zu 1.4 Sekunden. Ursache ist das Einfrieren der Transportverbindungen zu dem Zeitpunkt, an dem mit der Übertragung der Pufferinhalte zum neuen Transportgateway begonnen wird.

Ziel des entwickelten Verfahren ist es, die Unterbrechungszeiten der Transportverbindung, die durch das Einfrieren der Transportverbindung während der Migration der Statusinformation bedingt sind, zu reduzieren. Beim entwickelten Verfahren wird die Transportkommunikation nicht unmittelbar zu Beginn der Übertragung der Pufferinhalte zum neuen Transportgateway eingefroren, sondern erst zu einem späteren Zeitpunkt. Die Kommunikation in der Transportschicht wird parallel zur Migration der Statusinformation zugelassen. Das Verfahren wird als *nebenläufige Migration* bezeichnet. Der zeitliche Ablauf der nach einem Subnetzwechsel notwendigen Phasen einer Migration wird im folgenden genauer diskutiert. Darüber hinaus wird das Problem adressiert, daß sich die zu migrierenden Pufferinhalte bedingt durch die nebenläufig weiterhin stattfindende Transportkommunikation ändern können, während die Migration im Gange ist.

4.2.3.1 Zeitlicher Ablauf der nebenläufigen Migration

Zur Verdeutlichung des Konzeptes der nebenläufigen Migration wird es in Abb. 4.8 dem Konzept der Migration mit Einfrieren gegenübergestellt. Das Fast-Forwarding-Konzept, das für die nebenläufige Migration zwingend erforderlich ist, kann auch für die Migration mit Einfrieren angewandt werden. Aus diesem Grunde ist das Konzept der Migration mit Einfrieren kombiniert mit der Fast-Forwarding-Strategie ebenfalls in Abb. 4.8 mit aufgenommen. Für die drei verschiedenen Ansätze sind qualitativ die folgenden Zeitphasen dargestellt: Phase aktiver Transportkommunikation, Phase der Übertragung der Statusinformation und die Zeitdauer, während der die Transportkommunikation unterbrochen ist.

Zum Zeitpunkt $t = t0$ wechselt das mobile System in das neue Subnetz. Die Migration der Pufferinhalte zum neuen Transportgateway beginnt zum Zeitpunkt $t = t1$ und ist zum Zeitpunkt $t = t2$ bzw. $t = t2'$ abgeschlossen. Im Anschluß daran werden bis zum Zeitpunkt $t = t3$ bzw. $t = t3'$ die Protokollkontrollblöcke zum neuen Transportgateway übertragen.

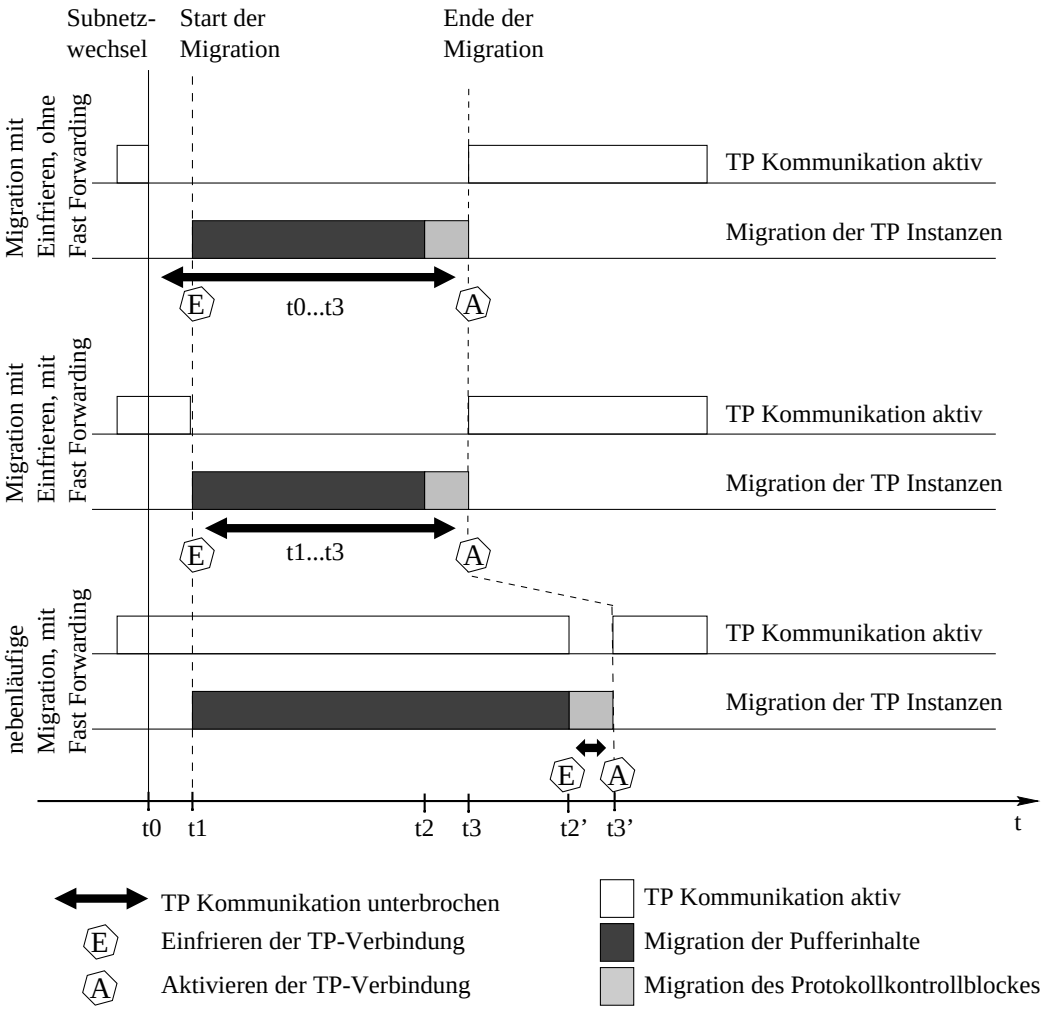


Abbildung 4.8: Nebenläufige Migration

Erfolgt die Migration ohne Einfrieren und kommt das Fast-Forwarding-Konzept nicht zum Einsatz, so ist die Transportkommunikation bereits ab dem Zeitpunkt $t = t0$ unterbrochen. Den Startzeitpunkt $t = t1$ der Migration der Pufferinhalte hinauszuzögern, macht somit keinen Sinn. Da auch während der Migration der Pufferinhalte keine Transportkommunikation möglich ist, ergibt sich insgesamt eine Unterbrechung der Kommunikation auf der Transportschicht während des Zeitraumes $[t0, t3]$.

Der wesentliche Vorteil, das Fast-Forwarding-Konzept zusammen mit der Migration mit Einfrieren einzusetzen, ist darin zu sehen, daß die Transportkommunikation während $[t0, t1]$ nicht unterbrochen, da das alte Transportgateway noch im Datenpfad liegt und somit noch als aktives Transportgateway fungieren kann. Hinsichtlich der durch die Migration der Transportinstanzen bedingten Unterbrechungsdauer ergeben sich durch das Fast-Forwarding-Konzept keine Vorteile.

Kernidee der nebenläufigen Migration ist es, die Übertragung der Pufferinhalte parallel zur gleichzeitig weiter stattfindenden Transportkommunikation zu realisieren. Um die nebenläufige Migration umsetzen zu können, ist es unbedingt notwendig, daß das Transportgateway im vorherigen Subnetz weiterhin als Transportgateway für die beiden zu migrierenden Transportinstanzen fungiert und somit auch nach dem Subnetzwechsel die Kommunikation in

der Transportschicht möglich ist. Das Fast-Forwarding-Konzept kann dies gewährleisten. Die Transportkommunikation ist bei dem Konzept der nebenläufigen Migration nicht nur im Zeitraum $[t0, t1]$, d.h. bis zum Start der Migration möglich, sondern bis zum Zeitpunkt $t = t2'$, zu dem ein identisches Abbild der Pufferinhalte bei dem neuen Transportgateway vorliegt. Zum Zeitpunkt $t = t2'$ wird die Verbindung eingefroren und werden die Protokollkontrollblöcke, z.B. der aktuelle Timeoutwert, die letzte bestätigte Sequenznummer usw., zum neuen Transportgateway migriert. Nach der Übertragung der Statusinformation zum Zeitpunkt $t = t3'$ werden die Verbindungen auf dem neuen Transportgateway wieder aktiviert. Gleichzeitig muß auch durch das Routing sichergestellt sein, daß ab diesem Zeitpunkt die Pakete über das neue Transportgateway übertragen werden.

Bei der Strategie mit Einfrieren ist die Unterbrechungsdauer von der Menge der aus den Sende- und Empfangspuffern der beiden zu migrierenden Transportinstanzen zu übertragenden Pufferinhalte abhängig. Diese wiederum hängt vom aktuellen Füllungsgrad der Sende- und Empfangspuffer der beiden Transportinstanzen auf dem Transportgateway zum Zeitpunkt des Migrationsstartes ab. Bei einer maximalen Puffergröße von 32 KByte [WS95] müssen im Falle komplett gefüllter Puffer 128 KByte an Pufferinhalten zum neuen Transportgateway migriert werden. Da die Transportkommunikation zu Beginn der Migration eingefroren und erst nach Abschluß der Migration wieder aktiviert wird, hat der aktuelle Pufferfüllungsgrad und somit auch die Menge der zu migrierenden Statusinformation einen direkten Einfluß auf die Dauer der Unterbrechung. In [BB95a] beschriebene Messungen für die Migration mit Einfrieren ergaben, daß vom Start der Migration zum Zeitpunkt $t = t1$ bis zum Ende der Migration zum Zeitpunkt $t = t3$ bis zu 1.4 Sekunden vergehen.

Wird hingegen die Statusinformation nebenläufig migriert, ist die Transportkommunikation lediglich während der Übertragung der beiden Transportprotokollkontrollblöcke, d.h. im Zeitraum $[t2', t3']$, unterbrochen. Die Grundidee der nebenläufigen Migration ist in [FZ97b] beschrieben. Eigene Messungen an einer prototypischen Realisierung sind in Kap. 5.2 und in [FZ97a], [FBZ97] beschrieben. Die Unterbrechungszeiten lassen sich mittels der nebenläufigen Migration auf konstant ca. 0.01 Sekunden reduzieren. Die nebenläufige Migration bietet somit den Vorteil kürzerer und konstanter Unterbrechungszeiten. Allerdings hat die nebenläufige Migration eine insgesamt längere Migrationsdauer im Vergleich zur Migration mit Einfrieren zur Folge. Ursache hierfür sind Veränderungen der Pufferinhalte der zu migrierenden Transportinstanzen, die sich wegen der nicht eingefrorenen Transportkommunikation ergeben können. Die Pufferinhalte, die sich seit dem Start der Migration verändert haben, müssen zusätzlich zum neuen Transportgateway übertragen werden.

4.2.3.2 Statusänderungen während der Migration

Der Aspekt sich zeitgleich mit der Migration verändernder Pufferinhalte wird exemplarisch an einem Sendepuffer diskutiert. Grundsätzlich sind von dieser Problematik sowohl der Sendepuffer als auch der Empfangspuffer der beiden in die indirekte Transportverbindung involvierten Transportinstanzen betroffen.

Abb. 4.9 verdeutlicht die Problematik sich verändernder Pufferinhalte während der Migration der Statusinformation. Betrachtet wird ein Sendepuffer mit von 1 bis 12 durchnumerierten Pufferplätzen einer zu migrierenden Transportinstanz auf dem Transportgateway. Pakete im Sendepuffer, die noch zum neuen Transportgateway zu migrieren sind, sind dunkelgrau dargestellt, hellgrau dargestellte Pakete sind bereits zum neuen Transportgateway übertragen

worden. Auf der Zeitachse sind die für die Migration relevanten Zeitpunkte dargestellt, wobei die Numerierung dieser Zeitpunkte analog zu Abb. 4.8 erfolgt. Durchgezogene und gestrichelte Pfeile repräsentieren Pakete, die Statusinformation, d.h. Pufferinhalte oder den Protokollkontrollblock, enthalten und vom alten Transportgateway an das neue Transportgateway gesendet werden. Gepunktet dargestellte Pfeile repräsentieren Bestätigungs-Pakete, die von der Partnertransportinstanz an die Transportinstanz, deren Sendepuffer in der Abbildung dargestellt ist, übertragen wurden. Abweichend von herkömmlichen Weg-Zeit-Diagrammen sind in der Abbildung nicht die zwischen zwei Partnertransportinstanzen ausgetauschten Pakete dargestellt, sondern lediglich die für die Migration des dargestellten Sendepuffers relevanten Pakete.

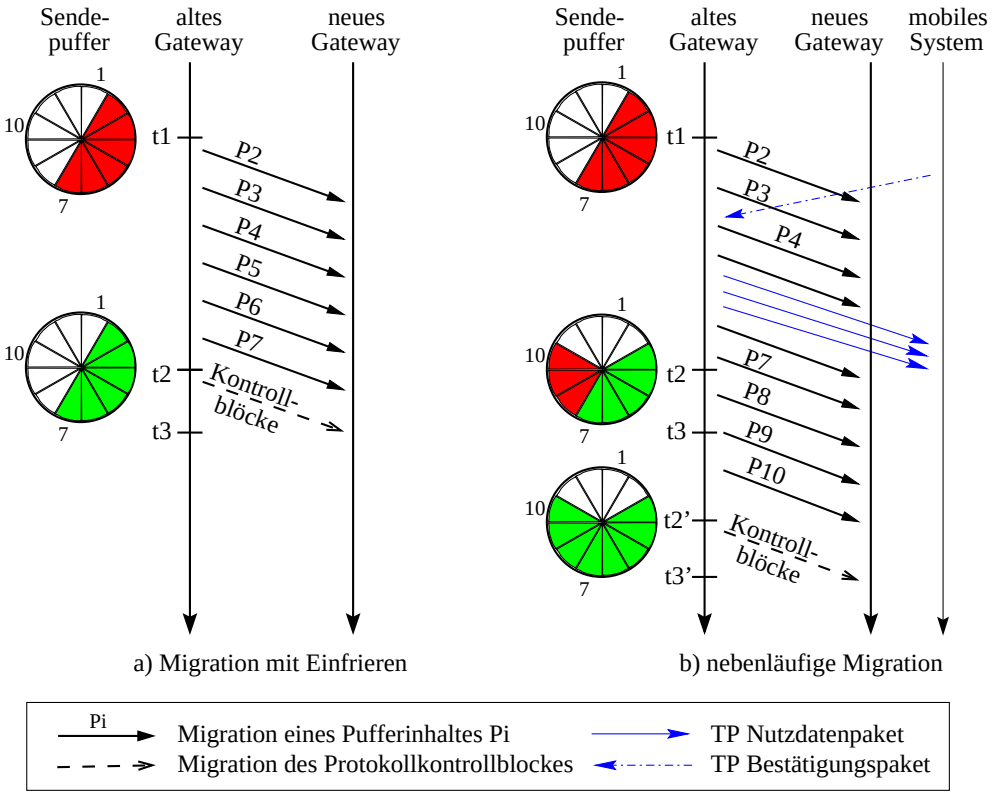


Abbildung 4.9: Statusänderungen während der Migration

Abb. 4.9a zeigt die Situation, falls die Transportinstanzen auf dem alten Transportgateway zu Beginn der Migration der Pufferinhalte eingefroren werden. Zum Zeitpunkt $t = t1$ befinden sich die Pakete $P2..P7$ im Sendepuffer. Die Transportkommunikation wird zu diesem Zeitpunkt eingefroren und mit der Migration der Pufferinhalte zu dem neuen Transportgateway begonnen. Zum Zeitpunkt $t = t2$ sind alle Pufferinhalte komplett zum neuen Transportgateway migriert worden. Da die Transportkommunikation eingefroren war, hat sich der Zustand bis zum Zeitpunkt $t = t2$ nicht verändert. Somit ist zu diesem Zeitpunkt beim neuen Transportgateway ein komplettes und identisches Abbild der Pufferinhalte des alten Transportgateways verfügbar. Nachdem der Transportprotokollkontrollblock zum neuen Transportgateway übertragen wurde, kann dort die Transportkommunikation zum Zeitpunkt $t = t3$ wieder aufgenommen werden.

Abb. 4.10 zeigt den Pseudocode für die Migration mit Einfrieren. Mit Großbuchstaben geschriebene Variablen bezeichnen Mengen und enthalten keine oder mehrere Nummern von

Pufferplätzen eines Sende- bzw. Empfangspuffers. Die Bezeichnung der wesentlichen Zeitpunkte tx ist analog zu den Bezeichnern in Abb. 4.9 gewählt. Wesentliches Merkmal der Migration mit Einfrieren ist, daß sich die Menge $BELEGTE\_PUFFER$ während der Migration nicht ändert und die Anzahl der in der Menge $ZU\_MIGRIERENDE\_PUFFER$ enthaltenen Elemente mit jeder Übertragung eines Pufferinhaltes streng monoton fällt.

```
t1:
  initialisiere BELEGTE_PUFFER mit aktueller Pufferbelegung
  ZU_MIGRIERENDE_PUFFER = BELEGTE_PUFFER

  solange ( ZU_MIGRIERENDE_PUFFER  nicht leer )
  {
    waehle NAECHSTER_PUFFER aus ZU_MIGRIERENDE_PUFFER
    migriere NAECHSTER_PUFFER
    entferne NAECHSTER_PUFFER aus ZU_MIGRIERENDE_PUFFER
  }

t2:
  migriere Protokollkontrollblock
t3:
```

Abbildung 4.10: Pseudocode für die Migration mit Einfrieren

Die sich im Falle der nebenläufigen Migration ergebende Situation ist in Abb. 4.9b dargestellt. Zum Startzeitpunkt der Migration enthält der Sendepuffer analog zum beschriebenen Szenario die Pakete $P2..P7$. Allerdings kann sich der Sendepuffer während der Übertragung der Pufferinhalte, d.h. im Zeitraum $[t1, t2]$ verändern, da die zugehörige Transportinstanz nicht eingefroren ist. Während dieses Zeitraumes trifft ein Bestätigungspaket der Partnerinstanz ein, das das Paket 2 bestätigt und das Löschen dieses Pakets aus dem Sendepuffer zur Folge hat. Darüber hinaus werden die Nutzdatenpakete $P8..P10$ von der betrachteten Transportinstanz an die Partnerinstanz übertragen. Insgesamt führt dies dazu, daß der Zustand des Sendepuffers zum Zeitpunkt $t = t2$ nicht identisch zu dem des Zeitpunktes $t = t1$ ist. Ohne weitere Maßnahmen wäre somit auf dem neuen Transportgateway kein identisches Abbild der zu migrierenden Transportinstanz verfügbar und könnte somit das neue Transportgateway nicht aktiviert werden. Bevor das neue Transportgateway aktiviert werden kann, müssen erst noch die Puffer $P8..P10$ zu diesem Gateway übertragen werden. Zum Zeitpunkt $t3'$ kann dann das neue Transportgateway aktiviert werden. Ein unnötig migrierter Puffer $P2$ und drei Puffer ($P8..P10$), die zusätzlich migriert werden müssen, ergeben sich in diesem Beispiel als Folge der nebenläufigen Migrationsstrategie. Ursache für die im Vergleich zur Migration mit Einfrieren längere Migrationsdauer sind diese zusätzlich zu migrierenden Pakete. Da aber bei der nebenläufigen Migration die Migrationsdauer nicht auch zugleich die Unterbrechungsdauer ist, ergibt sich aus der längeren Migrationsdauer nicht zwangsläufig eine längere Unterbrechungsdauer.

Der Pseudocode für die nebenläufige Migration ist in Abb. 4.11 aufgeführt. Da die Transportkommunikation nicht eingefroren ist, ändert sich die Menge $BELEGTE\_PUFFER$ und die Menge $ZU\_MIGRIERENDE\_PUFFER$ auch während der Migration. Insbesondere muß die Menge $ZU\_MIGRIERENDE\_PUFFER$ immer wieder neu bestimmt werden. Andernfalls würde die Migration der Puffer beendet, obwohl noch weitere Puffer zu migrieren wären.

```
t1:
  initialisiere BELEGTE_PUFFER mit aktueller Pufferbelegung
  leere MIGRIERTE_PUFFER
  ZU_MIGRIERENDE_PUFFER = BELEGTE_PUFFER

  solange ( ZU_MIGRIERENDE_PUFFER nicht leer )
  {
    waehle NAECHSTER_PUFFER aus ZU_MIGRIERENDE_PUFFER
    migriere NAECHSTER_PUFFER
    fuege NAECHSTER_PUFFER zu MIGRIERTE_PUFFER

    /* Pufferbelegung hat sich eventuell geaendert ! */
    initialisiere BELEGTE_PUFFER mit aktueller Pufferbelegung
    ZU_MIGRIERENDE_PUFFER = BELEGTE_PUFFER \ MIGRIERTE_PUFFER
  }

t2':
  migriere Protokollkontrollblock
t3':
```

Abbildung 4.11: Pseudocode für die nebenläufige Migration

Hinsichtlich der Ursachen für Änderungen der zu migrierenden Pufferinhalte während der nebenläufigen Migration muß zwischen Sendepuffern und Empfangspuffern einer Transportinstanz unterschieden werden. Änderungen der Sendepuffer können durch den Empfang von Bestätigungen der Partnertransportinstanz bedingt sein. Darüber hinaus werden neu gesendete Pakete für etwaige Übertragungswiederholungen zwischengespeichert und verändern somit ebenfalls den Sendepuffer. Änderungen der Empfangspuffer können durch den Empfang neuer Nutzdatenpakete oder durch die Entnahme korrekt empfangener Nutzdaten aus dem Empfangspuffer bedingt sein.

Terminieren der nebenläufigen Migration
Ändern sich die zu migrierenden Puffer schneller als die Pufferinhalte zum neuen Transportgateway migriert werden können, ist nicht sichergestellt, daß das beschriebene Verfahren terminiert. Aus diesem Grunde wird beim alten Transportgateway der Fortgang der Migration überwacht. Wird eine derartige Situation erkannt, wird eine Verlangsamung der Transportinstanzen oder sogar eine kurzzeitige temporäre Deaktivierung erzwungen. Somit kann das Terminieren des Verfahrens der nebenläufigen Migration gewährleistet werden.

4.2.4 Zusammenfassung

Das OMIT-Konzept stützt sich auf drei Säulen, um trotz der Mobilität von Endsystemen den indirekten Transportansatz unterstützen zu können: Eine geschickte Positionierung eines Transportgateways, das Fast-Forwarding-Konzept und das Konzept der nebenläufigen Migration. Indem das Transportgateway auf ausgewiesenen Systemen des Subnetzes realisiert wird

und zusätzlich das Fast-Forwarding-Konzept angewandt wird, kann die Anzahl der notwendigen Migrationen reduziert werden. Zentrale Idee des Fast Forwardings ist es, in der globalen Mobilitätsunterstützung dafür zu sorgen, daß die Pakete weiterhin über das alte Transportgateway geroutet und von dort zum aktuellen Aufenthaltsort des mobilen Systems weitergeleitet werden. Wesentliche Idee der nebenläufigen Migration ist es, während der Migration die Kommunikation in der Transportschicht nicht zu deaktivieren. Mittels dieser Strategie lassen sich – unabhängig von der Menge der zu migrierenden Statusinformation – die durch Migrationen bedingten Unterbrechungen auf konstant 10 ms reduzieren.

4.3 Architektur eines OMIT-Transportgateways

Die verschiedenen für die Realisierung eines Transportgateways auf einem Zwischensystem erforderlichen Komponenten sind Gegenstand der Betrachtungen in diesem Unterkapitel. Es wird sowohl auf Vorgänge, die innerhalb der Komponenten ablaufen, als auch auf die Interaktion zwischen den Komponenten eingegangen. Die Beschreibung der komponenteninternen Vorgänge beschränkt sich allerdings auf solche Komponenten, die zwar für die Realisierung eines Transportgateways erforderlich sind, die aber nicht direkt die Umsetzung des Fast-Forwarding-Konzeptes bzw. des Konzeptes der nebenläufigen Migration betreffen. Die Umsetzung dieser beiden Konzepte wird in Kapitel 4.4 bzw. Kapitel 4.5 im Detail vorgestellt.

4.3.1 Überblick über die Architektur eines Transportgateways

Der grundsätzliche Aufbau eines Transportgateways ist in Abb. 4.12 dargestellt. Von Details, die für das grundlegende Verständnis nicht erforderlich sind, wird abstrahiert. Sie werden im Anschluß an diesen Überblick diskutiert. Grau gekennzeichnet sind die Komponenten, die zusätzlich erforderlich werden oder modifiziert werden müssen, falls für mittels Mobile IP angebundene Endsysteme der indirekte Transportansatz inklusive der optimierten Mobilitätsunterstützung zum Einsatz kommen soll. Welche Komponenten in die Verarbeitung der Pakete indirekter Transportverbindungen involviert sind, verdeutlicht die graue Linie.

Selektion von Paketen indirekter Transportverbindungen
Pakete indirekter Transportverbindungen müssen in der IP-Schicht des Transportgateways als an die Transportinstanzen auszuliefernde Pakete identifiziert werden, obwohl sie nicht an das Transportgateway adressiert sind. Um die Entscheidung treffen zu können, ob ein Paket an eine Transportinstanz des Transportgateways auszuliefern ist, wird in der Komponente, die für die Selektion der Pakete verantwortlich ist, eine Liste indirekter Transportverbindungen verwaltet. Durch Vergleich der Adreßinformation eines empfangenen IP-Pakets mit der in der Liste gespeicherten Information kann entschieden werden, ob das Paket zu einer indirekten Transportverbindung gehört.

Steuerung der Zwischenpufferung
Pakete indirekter Transportverbindungen werden zwischengepuffert, falls die Transportinstanzen des Transportgateways, an die die Pakete auszuliefern sind, noch nicht für deren Bearbeitung bereit sind. Dies ist der Fall für Verbindungsaufbau- bzw. für Verbindungsabbaupakete

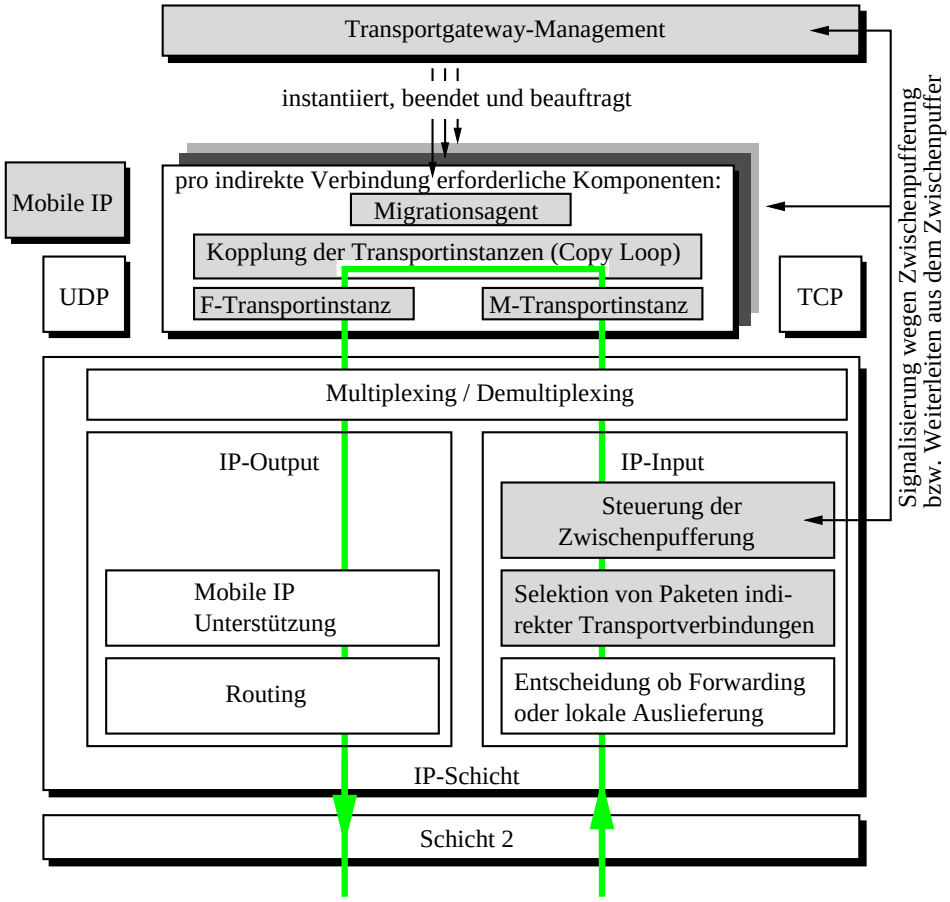


Abbildung 4.12: Architektur eines Transportgateways

des Transportprotokolls. Darüber hinaus müssen auch Pakete des Transportprotokolls, die bereits zum neuen Transportgateway geroutet werden, deren zugehörige Transportinstanz aber noch nicht aktiviert wurde, ebenfalls zwischengepuffert werden. Die Steuerung der Zwischenpufferung ist für die Pufferung, die Benachrichtigung anderer Komponenten und die Weiterleitung gepufferter Pakete verantwortlich. Aus dem Zwischenpuffer weitergeleitete Pakete werden vom Demultiplexer an die zugehörige Transportinstanz übergeben.

F-Transportinstanz und M-Transportinstanz
In diesen Transportinstanzen erfolgt die Protokollverarbeitung des jeweiligen Transportprotokolls. Bei der F-Transportinstanz handelt es sich um die Partnertransportinstanz des Festnetzrechners, d.h. in ihr ist das Transportprotokoll TCP realisiert. Die M-Transportinstanz ist die Partnertransportinstanz des mobilen Systems.

Kopplung der Transportinstanzen (Copy Loop)
Diese Komponente entnimmt korrekt empfangene und im Empfangspuffer der einen Transportinstanz abgelegte Nutzdaten und kopiert sie in den Sendepuffer der jeweils anderen Transportinstanz. Sie übernimmt somit die Kopplung der beiden Transportinstanzen.

Migrationsagent
Aufgabe des Migrationsagenten ist es, die Migration von Transportinstanzen zu steuern. Der Migrationsagent ist nur während einer Migration aktiv, aber nicht während des normalen Datentransfers. Sowohl auf dem alten als auch auf dem neuen Transportgateway ist der Migrationsagent in die Migration involviert. Die bereits skizzierten und in Kapitel 4.4.2 detailliert beschriebenen Mechanismen für die nebenläufige Migration werden im Migrationsagent realisiert.

Transportgateway-Management
Das Transportgateway-Management instantiiert, beendet und steuert die einzelnen für den Betrieb eines Transportgateway notwendigen Komponenten. Über neu einzurichtende indirekte Transportverbindungen wird das Management informiert. Es veranlaßt die Instantiierung der erforderlichen Transportinstanzen und der Copy Loop. Weiterhin empfängt es von mobilen Systemen gesendete Aufforderungen zur Migration von Transportinstanzen und delegiert die eigentliche Abwicklung der Migration an den Migrationsagenten.

Mobile IP
Das Fast-Forwarding-Konzept wird in Mobile IP integriert. Da es sich bei diesem Konzept um einen zentralen Beitrag der vorliegenden Arbeit handelt, wird es nicht in diesem Kapitel behandelt, sondern in Kapitel 4.5 im Detail präsentiert.

4.3.2 Modifikation existierender Komponenten

Wird der indirekte Transportansatz zusammen mit der optimierten Mobilitätsunterstützung eingesetzt, so sind einerseits zusätzliche Komponenten notwendig, andernfalls aber auch Änderungen an Komponenten vorzunehmen, die bei Verzicht auf den indirekten Ansatz nicht erforderlich wären. Die notwendigen Modifikationen an der IP-Schicht bzw. an Mobile IP werden im folgenden diskutiert.

4.3.2.1 Modifikationen in der IP-Schicht

Abb. 4.13 zeigt, wie in der IP-Schicht empfangene Pakete behandelt werden. Die dicken grauen Linien repräsentieren den Pfad von Paketen, die zu einer indirekten Transportverbindung gehören. Pakete, die nicht zu einer solchen Verbindung gehören, werden entlang der schwarzen, dünner eingezeichneten Linien transportiert.

Liste der indirekten Transportverbindungen
Die Liste der indirekten Transportverbindungen dient lediglich der Datenhaltung. Sie ist in der Komponente, in der die Selektion der Pakete indirekter Transportverbindungen vorgenommen wird, Grundlage für die Entscheidung, ob ein empfangenes IP-Paket regulär behandelt wird oder als ein Paket einer indirekten Transportverbindung identifiziert wird und dann speziell behandelt wird. In Abb. 4.14 sind zwei Typen von Listeneinträgen aufgeführt. Zum einen Listeneinträge, die existierende indirekte Transportverbindungen beschreiben, für die das Zwischensystem als Transportgateway fungiert. Zum anderen Einträge um festzulegen, welche

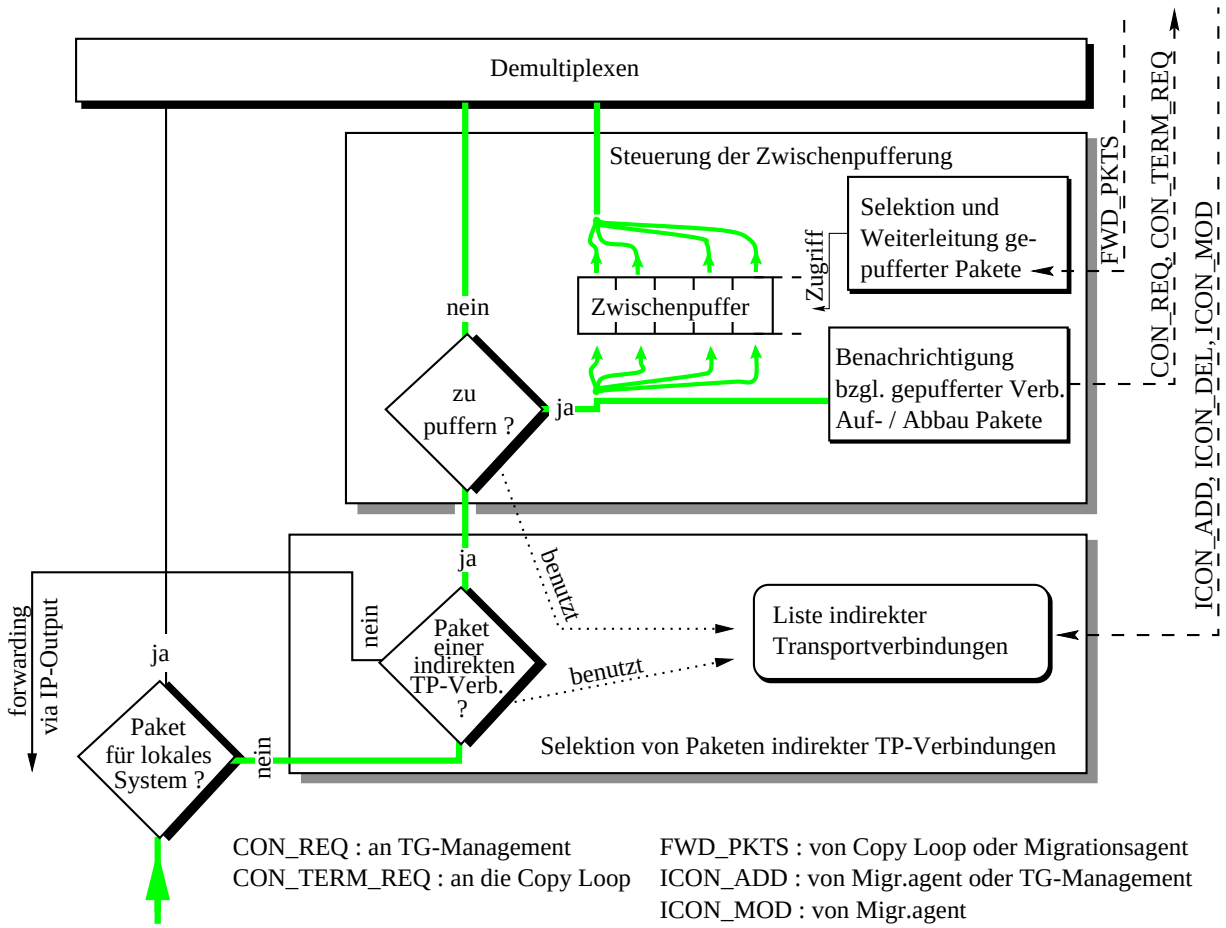


Abbildung 4.13: Datenpfad empfangener IP-Pakete

später neu etablierten indirekten Transportverbindungen das Zwischensystem als Transportgateways nutzen sollen. Neue Einträge werden in die Liste indirekter Transportverbindungen durch *ICON_ADD* Signale hinzugefügt, bestehende durch *ICON_DEL* Signale gelöscht bzw. durch *ICON_MOD* Signale geändert.

Die Einträge 1-4 zeigen indirekte Transportverbindungen, für die das Zwischensystem die Funktion des Transportgateways übernimmt. Die Identifikation erfolgt anhand des Fünf-Tupels (IP-Adresse 1, Port 1, IP-Adresse 2, Port 2, Protokoll). Da zwischen dem Transportgateway und dem Festnetzrechner bzw. dem Transportgateway und dem mobilen System ggf. verschiedene Transportprotokolle verwendet werden, kann das Protokollfeld zwei verschiedene Werte enthalten, die die jeweiligen verwendeten Transportprotokolle reflektieren. Zusätzlich ist für jede existierende indirekte Transportverbindung vermerkt, ob Pakete dieser Verbindung zwischenzupuffern sind. Pakete, die nicht zwischenzupuffern sind, werden direkt an den Demultiplexer übergeben.

Der fünfte Eintrag reflektiert, daß das Zwischensystem für neue indirekte Transportverbindungen, in die das Endsystem A involviert ist, als Transportgateway fungiert. Dies ist unabhängig davon, ob der Verbindungsaufbau von Endsystem A veranlaßt wird oder eine Verbindung zu dem Endsystem A aufgebaut werden soll. Da dieser Eintrag nicht eine einzelne Verbindung identifizieren soll, sind die Portnummern nicht von Bedeutung.

Das Zwischensystem kann auch für indirekte Transportverbindungen eines mobilen Sy-

Listen-eintrag	Verbindungstyp	IP-Adresse 1 (mobiles System)	Port 1	IP-Adresse 2	Port 2	Protokoll	zu_puffern
1	existierend	Endsystem A	5000	Endsystem Z	21	TP1 / TP2	0
2	existierend	Endsystem A	5010	Endsystem Z	20	TP1 / TP2	0
3	existierend	Endsystem B	5100	Endsystem Y	3000	TP1 / TP2	0
4	existierend	Endsystem C	5200	Endsystem X	3010	TP1 / TP2	1
5	neu	Endsystem A	-	-	-	TP1 / TP2	-

Abbildung 4.14: Liste indirekter Transportverbindungen

stems als Transportgateway operieren, obwohl es für neue Verbindungen dieses mobilen Systems nicht die Funktion des Transportgateways übernimmt. Die als Listeneintrag 3 bzw. 4 aufgeführten indirekten Verbindungen sind hierfür ein Beispiel. Für eine indirekte Verbindung des Endsystems B bzw. des Endsystems C dient das Zwischensystem als Transportgateway, obwohl es für neue Verbindungen dieser beiden Systeme nicht als Transportgateway fungiert.

Selektion von Paketen indirekter Transportverbindungen

Von der Schicht 2 an die IP-Schicht übergebene Pakete, die nicht an das lokale Systeme adressiert sind, sind potentiell Pakete, die zu einer indirekten Transportverbindung gehören. Sie werden unter Zuhilfenahme der Liste der indirekten Transportverbindungen identifiziert. Verbindungsaufbaupakete eines Transportprotokolls werden als Pakete einer indirekten Verbindung erkannt, falls entweder für die Quelladresse oder die Zieladresse des IP-Pakets ein Listeneintrag (Verbindungstyp neu) mit identischer IP-Adresse 1 in der Liste enthalten ist. Handelt es sich nicht um ein Verbindungsaufbaupaket, so wird es als ein Paket einer indirekten Verbindung erkannt, falls die Liste der indirekten Transportverbindungen einen Listeneintrag mit identischem Fünf-Tupel enthält. Pakete, die zu einer Verbindung gehören, für die das Zwischensystem als Transportgateway operiert, werden an die Steuerung der Zwischenpufferung weitergeleitet. Alle anderen Pakete werden zur weiteren Bearbeitung an IP-Output übergeben.

Steuerung der Zwischenpufferung

Ein zu einer indirekten Transportverbindung gehörendes Paket muß zwischengepuffert werden, falls die Transportinstanz, an die das Paket auszuliefern ist, noch nicht existiert, noch nicht aktiviert ist oder noch nicht bereit ist, das Paket zu verarbeiten. Für Verbindungsaufbaupakete erfolgt eine Zwischenpufferung, da diese Pakete erst weitergeleitet werden können, nachdem die Transportinstanzen instantiiert sind. Über gepufferte Verbindungsaufbaupakete wird das Transportgateway-Management mittels eines CON_REQ Signals informiert. Es veranlaßt daraufhin die Instantiierung der Transportinstanzen. Pakete, die weder einen Verbindungsaufbau noch einen Verbindungsabbau initiieren, werden gepuffert, falls die Notwendigkeit der Zwischenpufferung in der Liste der indirekten Transportverbindungen (siehe Abb. 4.14) vermerkt ist. Sie werden auf dem neuen Transportgateway bis zum Zeitpunkt der Aktivierung der Transportinstanzen zwischengepuffert. Eine Signalisierung bzgl. der Zwischenpufferung an andere Komponenten erfolgt nicht. Verbindungsabbaupakete werden ebenfalls gepuffert. Sie werden erst weitergeleitet, nachdem zuvor die zweite Teilverbindung terminiert wurde. Diese Terminierung wird von der Copy Loop veranlaßt, nachdem sie von der Steuerung der Zwischenpufferung mittels eines CON_TERM_REQ Signals über den bevorstehenden Verbin-

dungsabbau informiert wurde.

4.3.2.2 Modifikation an Mobile IP

Mobile IP muß dahingehend modifiziert werden, daß es das Fast-Forwarding-Konzept unterstützt. Da es sich bei diesem Konzept um eine wesentliche Komponente der optimierten Mobilitätsunterstützung für indirekte Transportansätze handelt, wird es nicht an dieser Stelle sondern in Kapitel 4.5 im Detail behandelt.

4.3.3 Zusätzlich erforderliche Komponenten

In Abb. 4.15 sind die Komponenten, die wegen der Verwendung des indirekten Transportansatzes zusätzlich erforderlich werden, durch einen grauen Schatten kenntlich gemacht. Es sind dies die beiden Transportinstanzen, die Copy Loop, der Migrationsagent und das Transportgateway-Management. Darüber hinaus sind die für die Interaktion zwischen den Komponenten ausgetauschten Signale mit aufgenommen und durch gestrichelte Pfeile dargestellt. Graue Pfeile zeigen, zwischen welchen Komponenten Pakete indirekter Transportverbindungen ausgetauscht werden. Entlang der dick eingezeichneten grauen Pfeile werden die Pakete weitergeleitet, mittels derer der Nutzdatentransfer zwischen den miteinander kommunizierenden Endsystemen realisiert wird. Während der Phase der Migration der Transportinstanzen wird entlang der dünnen grauen Pfeile die zu migrierenden Statusinformation transportiert.

4.3.3.1 Transportinstanzen

In den Transportinstanzen erfolgt die Protokollverarbeitung des jeweiligen Transportprotokolls. In der F-Transportinstanz wird das Transportprotokoll TCP verwendet, so daß die Interoperabilität zu den ebenfalls TCP verwendenden Kommunikationspartnern im Festnetz sichergestellt ist. In der M-Transportinstanz ist das gleiche Transportprotokoll realisiert wie im mobilen System. Da der Fokus nicht auf den intern in den Transportinstanzen eingesetzten Transportprotokollmechanismen liegt, wird auf sie nicht weiter eingegangen.

Die Migration von Transportinstanzen erfordert es, auf dem Transportgateway die Transportinstanzen indirekter Transportverbindungen einzufrieren bzw. wieder zu aktivieren. Der Migrationsagent stoppt bzw. startet mittels der Signale $STOP\_TPI$ und $START\_TPI$ die Protokollverarbeitung in den Transportinstanzen. Die Transportprotokollimplementierungen müssen aus diesem Grunde dahingehend modifiziert werden, daß sie bei Empfang dieser Signale die Protokollverarbeitung stoppen bzw. wieder aufnehmen.

4.3.3.2 Copy Loop

Aufgabe der Copy Loop ist es, die beiden Transportinstanzen zu koppeln. In der Phase des Verbindungsaufbaus bzw. Verbindungsabbaus einer indirekten Transportverbindung wird die Reihenfolge, in der die zwei Teilverbindungen aufgebaut bzw. abgebaut werden, von ihr gesteuert. Während der Datentransferphase ist sie für das Kopieren der Nutzdaten von der F-Transportinstanz zur M-Transportinstanz bzw. von der M-Transportinstanz zur F-Transportinstanz verantwortlich. Die vom Transportprotokoll nach dem korrekten Empfang im Emp-

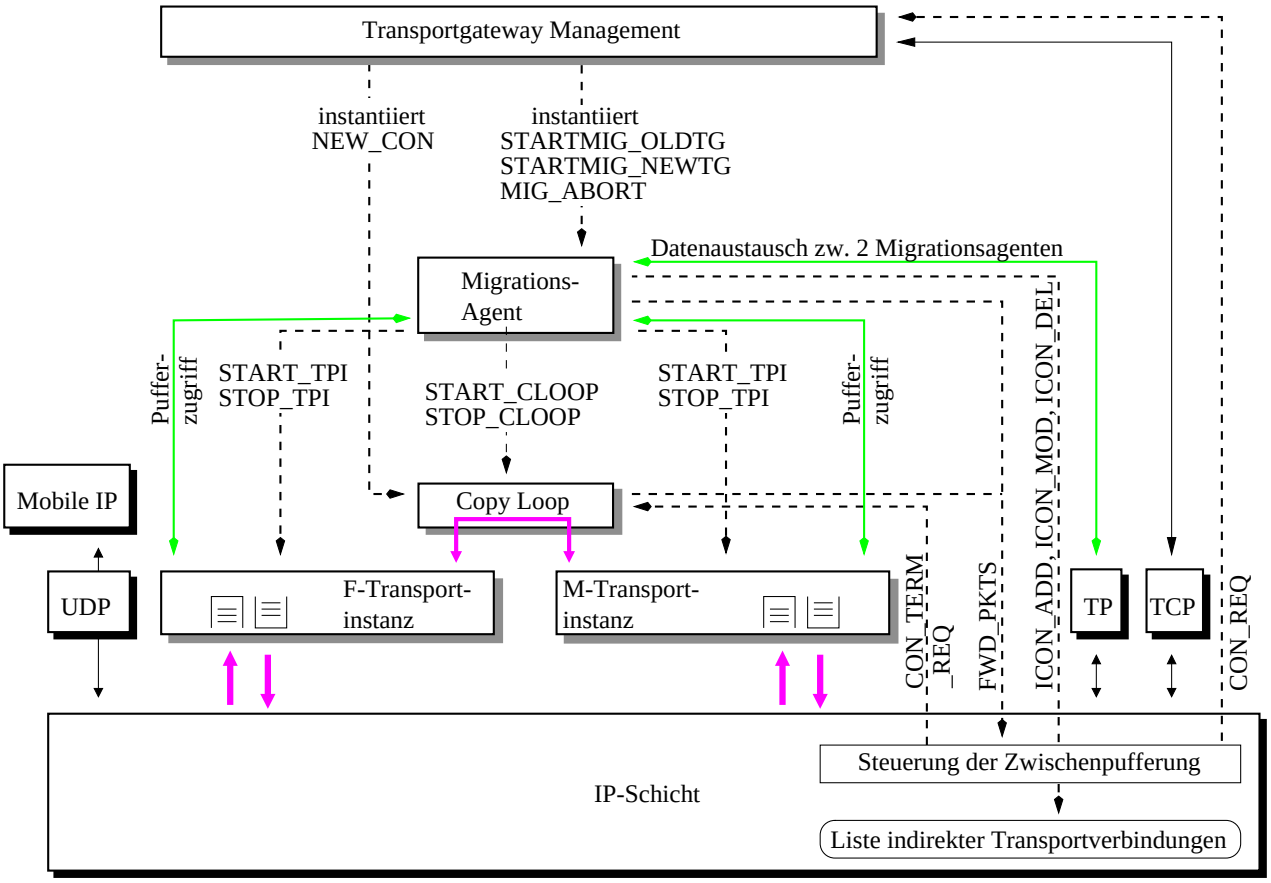
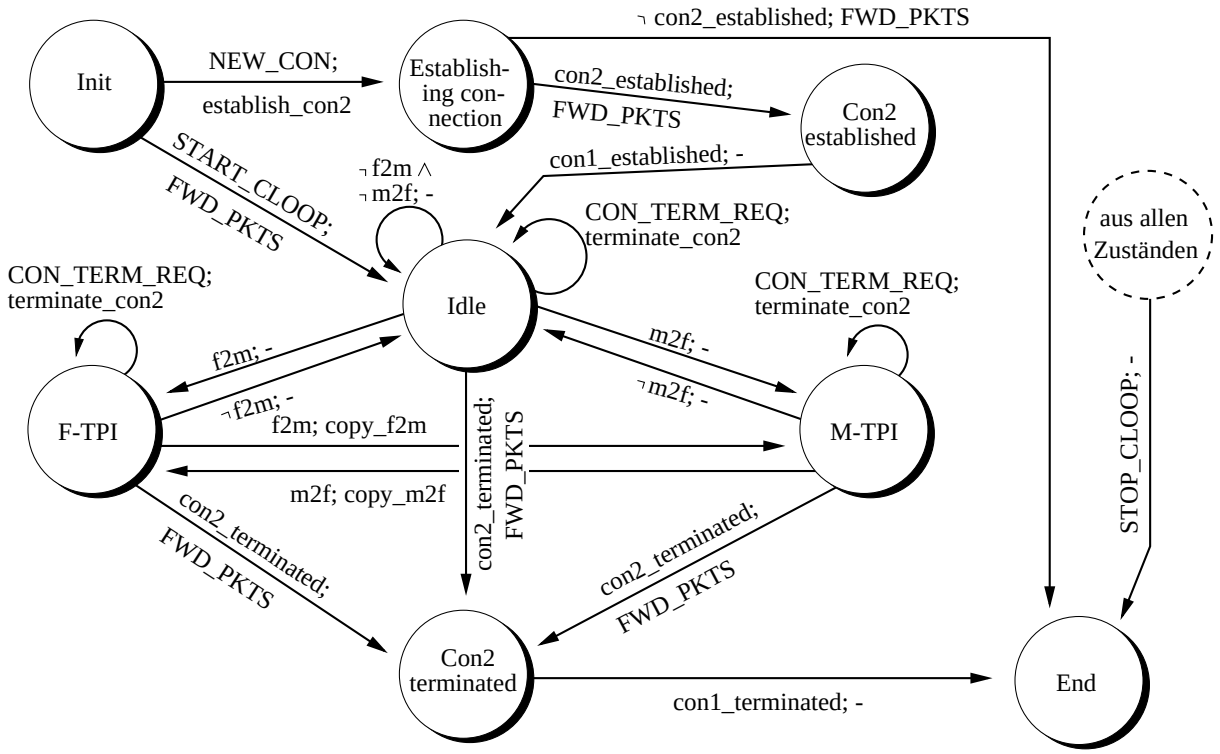


Abbildung 4.15: Datenfluß und Signalisierung zwischen den Komponenten

fangspuffer abgelegten Nutzdaten werden aus diesem Empfangspuffer entnommen und im Sendepuffer der jeweils anderen Transportinstanz abgelegt. Eine Zwischenpufferung der Daten erfolgt in der Copy Loop nicht, d.h. die Daten werden aus dem Empfangspuffer entnommen und unmittelbar danach im Sendepuffer abgelegt.

Die Copy Loop wird vom Transportgateway-Management instantiiert und durch das Signal *NEW_CON* über eine neu zu etablierende indirekte Transportverbindung informiert. Bezüglich des Terminierens einer Verbindung informiert die Steuerung der Zwischenpufferung mittels eines *CON_TERM_REQ* Signals. Das im Zuge einer Migration erforderliche Starten bzw. Stoppen der Copy Loop wird vom Migrationsagenten mittels der Signale *START_CLOOP* bzw. *STOP_CLOOP* veranlaßt.

Abb. 4.16 zeigt das Zustandsübergangsdiagramm für die Copy Loop. Für die Zustandsübergänge sind jeweils das Eingabeereignis und die Reaktionen in der Notation *Ereignis*; *Reaktion* aufgeführt. Mit Großbuchstaben bezeichnete Eingabeereignisse bzw. Reaktionen stehen für Signale, die von bzw. zu anderen Komponenten gesendet werden, Kleinbuchstaben kennzeichnen interne Eingabeereignisse bzw. Reaktionen. Die Zustände lassen sich in drei Gruppen unterteilen: Zustände für den Verbindungsaufbau der zwei Teilverbindungen („Init“, „Establishing connection“, „Con2 established“), während der Phase des Datentransfers relevante Zustände („Idle“, „F-TPI“, „M-TPI“) und Zustände, die für den Verbindungsabbau von Bedeutung sind („Con2 terminated“, „End“).



f2m : Empfangspuffer der F-Transportinstanz nicht leer UND Sendepuffer der M-Transportinstanz nicht voll
m2f : Empfangspuffer der M-Transportinstanz nicht leer UND Sendepuffer der F-Transportinstanz nicht voll

Abbildung 4.16: Zustandsübergangsdiagramm der Copy Loop

Verbindungsaufbau

Bei Empfang eines NEW_CON Signals wird der Aufbau der zweiten Teilverbindung veranlaßt (Reaktion $establish\_con2$) und aus dem Zustand „Init“ in den Zustand „Establishing connection“ gewechselt. Sobald diese Teilverbindung erfolgreich aufgebaut wurde (Ereignis $con2\_established$), wird die Transportinstanz, an die das Verbindungsaufbaupaket der ersten Teilverbindung adressiert ist, instantiiert, die Weiterleitung des im Zwischenpuffer gespeicherten Verbindungsaufbaupakets der ersten Teilverbindung mittels eines FWD_PKTS Signals veranlaßt und in den Zustand „Con2 established“ gewechselt. Konnte die zweite Teilverbindung nicht erfolgreich aufgebaut werden, wird die Transportinstanz nicht instantiiert, aber trotzdem die Weiterleitung des im Zwischenpuffer gespeicherten Verbindungsaufbaupakets durch ein FWD_PKTS Signal veranlaßt und in den Zustand „End“ gewechselt. Aus dem Zustand „Con2 established“ wird in den Zustand „Idle“ gewechselt, sobald auch die erste Teilverbindung etabliert ist (Ereignis $con1\_established$).

Datentransfer

Während der Phase des Datentransfers wird zwischen den Zuständen „Idle“, „F-TPI“ und „M-TPI“ gewechselt. Im Zustand „Idle“ befindet sich das System, falls keine Nutzdaten von der einen zur anderen Transportinstanz zu kopieren sind. Aus dem Zustand „M-TPI“ ist es möglich, Nutzdaten von der M-Transportinstanz zur F-Transportinstanz zu kopieren, aus dem Zustand „F-TPI“ können Nutzdaten von der F-Transportinstanz zur M-Transportinstanz

übertragen werden. Die Variable $f2m$ reflektiert, ob Daten von der F-Transportinstanz zur M-TPI kopiert werden können. Dies ist der Fall, falls der Empfangspuffer der F-Transportinstanz nicht leer ist und der Sendepuffer der M-Transportinstanz nicht voll ist. Ob Daten von der M-Transportinstanz zur F-TPI kopiert werden können, gibt die Variable $m2f$ wieder.

Das System verbleibt im Zustand „Idle“, falls die Auswertung der Variablen $f2m$ und $m2f$ ergibt, daß zwischen den Transportinstanzen keine Nutzdaten zu kopieren sind. Wird anhand der Auswertung der Variable $f2m$ erkannt, daß Daten von der F-Transportinstanz zur M-Transportinstanz kopiert werden können, wird in den Zustand „F-TPI“ gewechselt. Die Copy Loop wechselt aus diesem Zustand weiter in den Zustand „M-TPI“ und kopiert Nutzdaten (Reaktion $copy\_f2m$) von der F-Transportinstanz zur M-Transportinstanz. Ergibt im Zustand „M-TPI“ die Auswertung der Variable $m2f$, daß Nutzdaten von der M-Transportinstanz zur F-Transportinstanz zu kopieren sind, werden diese kopiert (Reaktion $copy\_m2f$) und in den Zustand „F-TPI“ gewechselt. Ist dies nicht der Fall, wird in den Zustand „Idle“ gewechselt.

Sind in beide Richtungen Nutzdaten zu kopieren, so wechselt der Automat zwischen den Zuständen „F-TPI“ und „M-TPI“. Somit ist sichergestellt, daß abwechselnd aus der F-Transportinstanz bzw. der M-Transportinstanz Nutzdaten kopiert werden. Auch das Kopieren in nur einer einer Richtung wird unterstützt. Sind beispielsweise nur Nutzdaten von der F-Transportinstanz zur M-Transportinstanz zu kopieren, so ergeben sich folgende Zustandsübergänge: „F-TPI“ → „M-TPI“ → „Idle“ → „F-TPI“ → „M-TPI“ → „Idle“ usw.

Verbindungsabbau
Wird von einer der beiden miteinander kommunizierenden Endsysteme ein Verbindungsabbau veranlaßt, so wird das Verbindungsabbaupaket zwischengepuffert und die Copy Loop mittels eines CON_TERM_REQ Signals darüber informiert. Bei Eintreffen dieses Signals kann sich die Copy Loop in einem der drei Zustände „Idle“, „F-TPI“ oder „M-TPI“ befinden. Das System initiiert die Terminierung der zweiten Verbindung (Reaktion $terminate\_con2$), verbleibt aber im gleichen Zustand. Solange der Abbau dieser zweiten Verbindung noch nicht abgeschlossen ist, kopiert die Copy Loop noch Daten zwischen den Transportinstanzen. Sobald der Verbindungsabbau der zweiten Verbindung vollzogen ist (Reaktion $con2\_terminated$), wechselt das System in den Zustand „Con2 terminated“ und signalisiert (Reaktion FWD_PKTS) an die Zwischenpufferung, daß das gepufferte Verbindungsabbaupaket weiterzuleiten ist. Ist auch die erste Verbindung terminiert, wird in den Zustand „End“ gewechselt.

4.3.3.3 Migrationsagent

Der Fokus der folgenden Betrachtungen liegt auf der Interaktion des Migrationsagenten mit den anderen Komponenten eines Transportgateways. Die in ihm realisierten Verfahren und Strategien für eine nebenläufige Migration der Pufferinhalte werden in Kapitel 4.4 im Detail diskutiert.

Der Migrationsagent wird vom Transportgateway-Management, wie in Abb. 4.15 dargestellt, instantiiert. Das Management startet auch die Migration. Der Migrationsagent auf dem alten, noch aktiven Transportgateway wird durch das $STARTMIG\_OLDTG$ Signal gestartet, der auf dem neuen Transportgateway durch das $STARTMIG\_NEWTG$ Signal. Kann das neue Transportgateway aktiviert werden, so informiert der Agent durch ein FWD_PKTS Signal die Steuerung der Zwischenpufferung darüber, daß zwischengepufferte Pakete weitergeleitet

werden können. Darüber hinaus informiert er mittels *START_TPI* bzw. *STOP_TPI* Signalen die Transportinstanzen darüber, wann die Protokollverarbeitung zu starten bzw. zu stoppen ist. Um die Daten zum neuen Transportgateway migrieren zu können, ist sowohl im alten als auch im neuen Transportgateway der Zugriff auf die Sendepuffer und die Empfangspuffer der Transportinstanzen erforderlich.

Abb. 4.17 zeigt das Zustandsübergangsdiagramm für den Migrationsagenten und verdeutlicht zugleich, zu welchen Zeitpunkten welche Signale an andere Komponenten gesendet werden bzw. von diesen empfangen werden. Die in der oberen Hälfte dargestellten Zustände sind Zustände, die im alten Transportgateway von Bedeutung sind. In der unteren Hälfte dargestellte Zuständen sind auf dem neuen Transportgateway relevant.

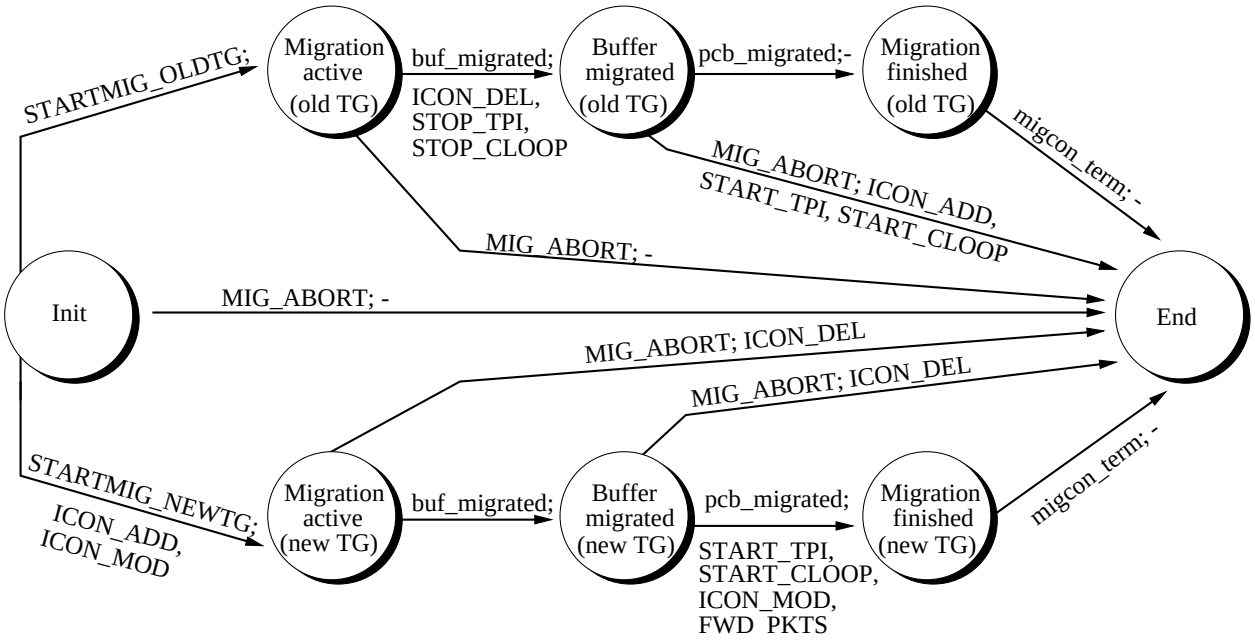


Abbildung 4.17: Zustandsübergangsdiagramm des Migrationsagenten

Die einzelnen Zustände des Zustandsübergangsdiagramms reflektieren die verschiedenen Phasen der nebenläufigen Migration, die bereits in Kapitel 4.2.3 anhand von Abb. 4.8 diskutiert wurden. Tabelle 4.4 kann entnommen werden, zu welchen Zeitpunkten der nebenläufigen Migration sich der Automat in welchem Zustand befindet. Die für die Identifikation der Zeitpunkte verwendeten Bezeichner sind analog zu denen in Abb. 4.8 gewählt.

Zustand	Zeitraum
Migration active	[t1,t2']
Buffer migrated	[t2',t3']
Migration finished	[t3',...]

Tabelle 4.4: Zuordnung der Zustände zu den Phasen der nebenläufigen Migration

Im Zustand „Migration active (old TG)“ werden die Pufferinhalte zum neuen Transportgateway übertragen. Sobald alle Puffer zum neuen Transportgateway übertragen wurden (Ereignis *buf_migrated*), werden die Transportinstanzen eingefroren (Reaktion *STOP_TPI*), die Copy Loop gestoppt (Reaktion *STOP_CLOOP*) und die Verbindung aus der Liste der indirekten Verbindungen entfernt (Reaktion *ICON_DEL*). Pakete dieser Verbindung werden

somit nicht mehr an die Transportinstanz ausgeliefert. Weiterhin wird in den Zustand „Buffer migrated (old TG)“ gewechselt. Nachdem auch der Protokollkontrollblock migriert ist, wird in den Zustand „Migration finished (old TG)“ gewechselt.

Bei Empfang des *STARTMIG_NEWTG* Signals wird im neuen Transportgateway die Verbindung zur Liste der indirekten Verbindungen hinzugefügt (Reaktion *ICON_ADD*) und vermerkt (Reaktion *ICON_MOD*), daß Pakete dieser indirekten Transportverbindung zu puffern sind. Anschließend erfolgt ein Wechsel in den Zustand „Migration active (new TG)“. In diesem Zustand empfängt das Transportgateway die migrierten Puffer. Hat es alle zu migrierenden Puffer empfangen (Ereignis *buf_migrated*), wechselt es in den Zustand „Buffer migrated (new TG)“. Sobald auch der Protokollkontrollblock beim neuen Transportgateway verfügbar ist (Ereignis *pcb_migrated*), werden die Copy Loop und die Transportinstanzen gestartet (Reaktionen *START_TPI*, *START_CLOOP*), die Listeneinträge dahingehend modifiziert (Reaktion *ICON_MOD*), daß Pakete dieser Verbindung nicht mehr zu puffern sind, die Weiterleitung gepufferter Pakete veranlaßt (Reaktion *FWD_PKTS*) und anschließend in den Zustand „Migration finished (new TG)“ gewechselt. Sobald die Verbindung zwischen dem Migrationsagenten des alten Transportgateways und dem des neuen Transportgateways, über die die zu migrierenden Daten gesendet werden, beendet ist (Ereignis *migcon_term*), wird in den Zustand „End“ gewechselt.

Wird die Migration abgebrochen (Ereignis *MIG_ABORT*), müssen die Aktionen teilweise wieder rückgängig gemacht werden. Im alten Transportgateway wird die Verbindung wieder in die Liste der indirekten Verbindungen aufgenommen (Reaktion *ICON_ADD*) und werden die Transportinstanzen und die Copy Loop wieder gestartet (Reaktionen *START_TPI*, *START_CLOOP*). Im neuen Transportgateway wird die Verbindung aus der Liste der indirekten Transportverbindungen entfernt (Reaktion *ICON_DEL*).

4.3.3.4 Transportgateway-Management

Falls ein Transportgateway für ein bestimmtes mobiles System für neue indirekte Transportverbindungen als Transportgateway fungieren soll, wird das Transportgateway-Management von diesem mobilen System darüber informiert. Es veranlaßt daraufhin mittels eines *ICON_ADD* Signals das Hinzufügen eines neuen Listeneintrages (Verbindungstyp = neu) zur Liste der indirekten Transportverbindungen (siehe Abb. 4.14). Soll ein Transportgateway für neue Verbindungen nicht mehr als Transportgateway arbeiten, so wird der zugehörige Listeneintrag mittels *ICON_DEL* gelöscht.

Das Transportgateway-Management wird mittels eines *CON_REQ* Signals von der Steuerung der Zwischenpufferung über eine neu aufzubauende indirekte Verbindung informiert. Es instantiiert daraufhin die Copy Loop und veranlaßt mittels eines *NEW_CON* Signals an die Copy Loop den Verbindungsaufbau.

Soll eine Migration gestartet werden, so wird das Transportgateway-Management vom mobilen System darüber in Kenntnis gesetzt. Daraufhin veranlaßt es die Instantiierung des Migrationsagenten und startet diesen. Der Abbruch einer Migration wird ebenfalls vom mobilen System initiiert und an das Management der involvierten Transportgateways gemeldet. Das Management veranlaßt daraufhin mittels eines *MIG_ABORT* Signals den Migrationsagenten, die Migration abzubrechen.

4.4 Nebenläufige Migration der Statusinformation

Die Statusinformation in einer Transportinstanz setzt sich aus den Pufferinhalten und dem Transportprotokollkontrollblock zusammen. Sie kann entweder mittels der nebenläufigen Migration oder durch die Migration mit Einfrieren dem neuen Transportgateway verfügbar gemacht werden. Im folgenden wird der Ablauf der nebenläufigen Migration, deren Grundkonzept und deren Vorteile gegenüber der Migration mit Einfrieren bereits in Unterkapitel 4.2.3 diskutiert wurden, im Detail betrachtet. Der Fokus liegt auf den für die nebenläufige Migration der Statusinformation notwendigen Mechanismen und den zusätzlich erforderlichen Komponenten. Eine nebenläufige Migration ist nur dann möglich, falls trotz eines Subnetzwechsels die Transportkommunikation nicht unterbrochen ist. Das Fast Forwarding, das dies sicherstellt, wird bei den folgenden Ausführungen zur nebenläufigen Migration als realisiert vorausgesetzt.

4.4.1 Komponenten für die nebenläufige Migration

Abb. 4.18 zeigt auf der linken Seite das alte – noch aktive – Transportgateway und auf der rechten Seite das neue – passive, d.h. noch nicht aktivierte – Transportgateway, auf das die Transportinstanzen migriert werden sollen. Für die Migration ist ein Migrationsagent und ein Transportsystem (TCP/UDP) für die Übertragung der Statusinformation erforderlich. Die Pufferselektion erfolgt im Migrationsagent auf Basis der realisierten Migrationsstrategie. Bei der Migration sind der Sendepuffer und der Empfangspuffer beider Transportinstanzen, d.h. insgesamt vier Puffer zu betrachten. Belegte Pufferplätze sind grau dargestellt, nicht belegte weiß. Die Migration ist im dargestellten Szenario schon im Gange, d.h. eine Teilmenge der sich auf dem aktiven Transportgateway im Sende- bzw. Empfangspuffer befindenden Nutzdaten ist bereits zum passiven Transportgateway übertragen worden. Der für den Fortgang der Transportkommunikation erforderliche Datentransport ist mittels schwarzer Pfeile dargestellt, graue Pfeile repräsentieren den für die Migration der Transportinstanzen notwendigen Zugriff auf die Statusinformation und die Übertragung der Statusinformation.

Migrationsagent
Die Migrationsagenten des aktiven und des passiven Transportgateways kommunizieren miteinander. Zwischen ihnen wird die zu migrierende Statusinformation und Information bzgl. des Fortgangs der Migration ausgetauscht. Ein Migrationsagent hat sowohl lesenden als auch schreibenden Zugriff auf die Sende- und Empfangspuffer und den Protokollkontrollblock der zu migrierenden Transportinstanzen. Darüber hinaus hat er auch Kenntnis davon, welche Puffer auf dem aktiven Transportgateway belegt sind oder ggf. nach dem Empfang einer Bestätigung von der Partnerinstanz des Transportprotokolls bereits wieder freigegeben wurden. Der Migrationsagent kann also jederzeit entscheiden, welche Pufferinhalte bereits migriert wurden oder erst noch migriert werden müssen. Auch die Reihenfolge, in der die Pufferinhalte zum passiven Transportgateway migriert werden, obliegt der Entscheidung des Migrationsagenten. Diese sogenannte *Puffermigrationsstrategie* hat entscheidenden Einfluß auf die Dauer der Migration und die Menge der unnötig migrierten Statusinformation. Über das Transportsystem kommunizieren die beiden Migrationsagenten miteinander.

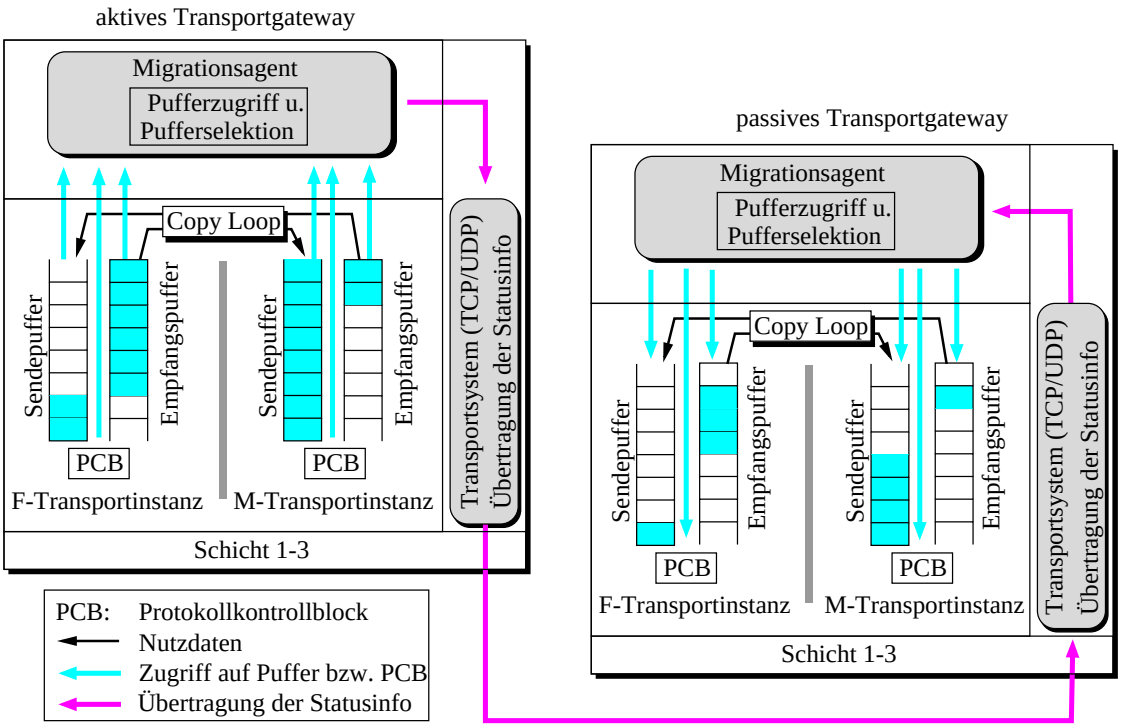


Abbildung 4.18: Komponenten für die nebenläufige Migration

Transportsystem für die zu migrierende Statusinformation
Für die Übertragung der zu migrierenden Statusinformation von dem alten, aktiven Transportgateway zu dem neuen, passiven Transportgateway ist ein zuverlässiger Datentransport zwischen diesen beiden Systemen erforderlich. Prinzipiell bieten sich zwei Möglichkeiten an, um die erforderliche zuverlässige Datenkommunikation zwischen den beiden Transportgateways zu realisieren:

- Nutzung des zuverlässigen Datendienstes von TCP oder
- Implementierung eigener Zuverlässigkeitsmechanismen im Migrationsagenten.

Das Aufsetzen auf dem zuverlässigen Datendienst von TCP bietet den Vorteil eines geringeren Implementierungsaufwandes und eines schlankeren Migrationsagenten. Es muß besonderes Augenmerk bei der Bewertung dieser beiden Varianten auf der für die Migration notwendigen Gesamtdauer liegen. Hier zeigt sich, daß sich bedingt durch die Slow-Start-Mechanismen von TCP Verzögerungen ergeben. Auch die ggf. notwendige Übertragungswiederholung eines TCP-Pakets, das zu migrierende Statusinformation transportiert, wird unnötig lange verzögert, falls auf den Ablauf des zugehörigen TCP-Timers gewartet werden muß.

Sind die für die zuverlässige Migration der Daten notwendigen Mechanismen im Migrationsagenten realisiert, so läßt sich die Gesamtdauer der Migration reduzieren, da die Mechanismen, die die Zuverlässigkeit der Übertragung sicherstellen, speziell auf die Anforderungen der Migration der Pufferinhalte abgestimmt werden können. Es müssen nämlich nur die Pufferinhalte, die zum Zeitpunkt, zu dem das neue Transportgateway aktiviert wird, in den Transportinstanzen des alten Transportgateways gespeichert sind, zu dem neuen Transportgateway übertragen werden. Während also im Falle der Nutzung des zuverlässigen Datendienstes von

TCP generell die gesamte Statusinformation zuverlässig übertragen wird, d.h. ggf. wiederholt wird, kann der Migrationsagent mit seinem Wissen über den aktuellen Zustand der Sende- und Empfangspuffer, die Übertragungswiederholung auf die Statusinformation beschränken, die sich auch wirklich zum Zeitpunkt der potentiellen Übertragungswiederholung im jeweiligen Puffer befindet.

4.4.2 Puffermigrationsstrategien

In welcher Reihenfolge die zu migrierenden Puffer zum neuen Transportgateway übertragen werden, wird in diesem Abschnitt diskutiert. Weiterhin wird die explizite Migrationsstrategie der impliziten Migrationsstrategie gegenübergestellt. Bei der expliziten Strategie werden alle zur Statusinformation gehörenden Pufferinhalte mittels des Transportsystems zum neuen Transportgateway übertragen. Bei der impliziten Migration wird nur ein Teil der zu migrierenden Daten über das Transportsystem gesendet. Aus diesem Grunde erfordert die implizite Migration weniger Ressourcen als die explizite Migration.

4.4.2.1 Mobiles System als Datenquelle bzw. Datensenke

Grundsätzlich muß bei Betrachtung des Pufferfüllungsgrades der zu migrierenden Transportinstanzen berücksichtigt werden, in welche Richtung Nutzdaten gesendet werden. In Abhängigkeit davon, ob das mobile System Datenquelle oder Datensenke ist, ergeben sich grundlegend verschiedene Situationen. Ursache hierfür sind die Unterschiede hinsichtlich der im Festnetz bzw. im drahtlosen Netz verfügbaren Bandbreiten.

In der Regel wird die drahtlose Teilstrecke eine geringere Übertragungsbandbreite bereitstellen als die drahtgebundene. Als unmittelbare Folge ergibt sich, daß für den Mobilteilnehmer bestimmte Nutzdaten im Transportgateway von der F-Transportinstanz schneller empfangen werden, als sie von der M-Transportinstanz an das mobile System gesendet werden können. Als Konsequenz bildet sich eine verteilte Warteschlange, d.h. der Empfangspuffer der F-Transportinstanz und der Sendepuffer der M-Transportinstanz füllen sich. Der Empfangspuffer der M-Transportinstanz und der Sendepuffer der F-Transportinstanz enthalten hingegen in der Regel keine oder nur wenige Nutzdaten.

Da der für die Migration der Pufferinhalte notwendige Aufwand direkt abhängig vom Füllungsgrad der Puffer zum Zeitpunkt des Starts des Migration ist, bestimmen im wesentlichen der Empfangspuffer der F-Transportinstanz und der Sendepuffer der M-Transportinstanz die Migrationsdauer. Aus diesem Grunde liegt der Fokus bei den weiteren Betrachtungen auf der Migration dieser Pufferinhalte. Der Inhalt der beiden anderen Puffer muß zwar auch migriert werden, fällt aber wegen der geringen Menge darin enthaltener Nutzdaten nicht wesentlich ins Gewicht.

4.4.2.2 Reihenfolge der Migration der Puffer

Die Reihenfolge, in der die in den Puffern gespeicherten Nutzdaten zum passiven Transportgateway übertragen werden, kann prinzipiell vom Migrationsagenten beliebig gewählt werden. Allerdings hat die Auswahlreihenfolge Einfluß auf die Menge der zu migrierenden Nutzdaten und somit auch auf die Migrationsdauer. In Abb. 4.19 ist eine aktuelle Pufferbelegung

für eine vom Festnetzsender zum mobilen Endsystem gerichtete Datenkommunikation dargestellt. Die Pufferplätze sind sequentiell durchnumeriert. Diese Numerierung ist nicht mit den von den Transportinstanzen verwendeten und in den Paketen des Transportprotokolls kodierten Sequenznummern zu verwechseln. Sie dient lediglich dazu, im betrachteten Szenario die Pufferplätze eindeutig zu identifizieren. Sowohl im Empfangspuffer als auch im Sendepuffer werden Pufferplätze mit einer niedrigeren Sequenznummer vor Plätzen mit einer höheren Sequenznummer gefüllt.

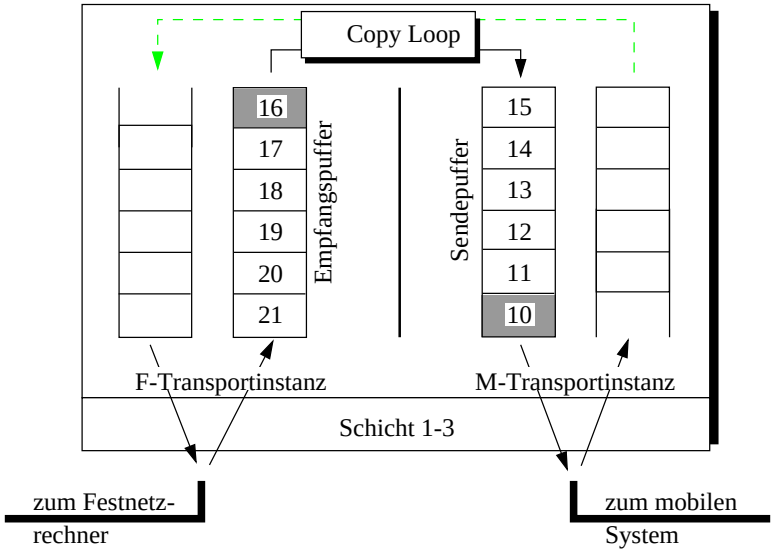


Abbildung 4.19: Reihenfolge der Puffermigration

Der Inhalt des Pufferplatzes mit der Nummer 10 wird vor allen anderen aus dem Sendepuffer der M-Transportinstanz gelöscht, da dieser Pufferplatz die als nächstes vom mobilen System zu bestätigenden Nutzdaten enthält. Werden die Nutzdaten bestätigt, wird der Inhalt des Pufferplatzes gelöscht und ein Pufferplatz verfügbar. Die Copy Loop kopiert daraufhin den Inhalt des Pufferplatzes 16 in den Sendepuffer der M-Transportinstanz und löscht ihn aus dem Empfangspuffer der F-Transportinstanz. Es ist unmittelbar einsichtig, daß es im skizzierten Szenario nicht sinnvoll ist, die in Pufferplatz 10 bzw. 16 gespeicherten Nutzdaten zu migrieren, da sie nach dem Löschen nicht mehr im jeweiligen Puffer sind und somit auch nicht mehr zur zu migrierenden Statusinformation gehören. Die Migration wäre unnötig. Der Inhalt von Pufferplätzen mit einer niedrigen Sequenznummer wird vor dem Inhalt von Pufferplätzen mit einer höheren Sequenznummer gelöscht. Damit tritt für Pufferplätze mit niedriger Sequenznummer früher und auch mit einer höheren Wahrscheinlichkeit der Fall ein, daß sie aufgrund der weiterhin aktiven Transportkommunikation nach Empfang entsprechender Bestätigungen gelöscht werden, als für Pufferplätze mit einer höheren Sequenznummer. Umgekehrt sind die Nutzdaten in einem Puffer mit einer hohen Sequenznummer diejenigen Daten, die am längsten im jeweiligen Puffer verbleiben. Aus diesem Grunde ist es sinnvoll, den Inhalt von Pufferplätzen mit hohen Sequenznummern zeitlich vor dem Inhalt von Pufferplätzen mit niedrigen Sequenznummern zu migrieren.

Als Migrationsstrategie ergibt sich das folgende Verfahren: Steht der Migrationsagent vor der Aufgabe, in den Puffern gespeicherte Nutzdaten vom aktiven auf das passive Transportgateway zu migrieren, so wählt er zunächst mittels Round Robin einen der zwei Empfangspuffer bzw. zwei Sendepuffer aus. Sind bereits alle Pufferplätze des ausgewählten Puffers migriert,

so wird mittels Round Robin der nächste der zwei Empfangspuffer bzw. zwei Sendepuffer selektiert. Sind noch nicht alle Pufferplätze des ausgewählten Puffers migriert, so wird aus der Menge der noch nicht migrierten Pufferplätze derjenige mit der höchsten Sequenznummer ausgewählt. Der Inhalt dieses Pufferplatzes wird als nächstes migriert.

4.4.2.3 Explizite vs. implizite Migration

Unter der *expliziten Migration* ist die vom Migrationsagenten veranlaßte Übertragung von Pufferinhalten zum passiven Transportgateway zu verstehen. Die Pufferinhalte werden hierzu in einer *gesonderten Übertragung* über das Transportsystem (siehe Abb. 4.18) vom Migrationsagenten des alten Transportgateways zum Migrationsagenten des neuen, passiven Transportgateways gesendet. Für die Übertragung ist zusätzliche Übertragungsbandbreite notwendig.

Bei der *expliziten Migration* werden im Sendepuffer der M-Transportinstanz gespeicherte Nutzdaten zum Teil zweifach auf der Strecke zwischen dem altem und dem neuen Transportgateway übertragen: Zum einen wegen der weiterhin aktiven Transportkommunikation zwischen dem Transportgateway und dem mobilen System, zum anderen – da die im Puffer gespeicherten Nutzdaten auch zur zu migrierenden Statusinformation gehören – durch gesonderte Übertragung vom Migrationsagenten des alten Transportgateways zum Migrationsagenten des neuen Transportgateways. Kernidee der impliziten Migration ist es, diese doppelte Übertragung zwischen alten und neuem Transportgateway zu vermeiden.

Bei der *impliziten Migration* werden Transportdateneinheiten, die von der M-Transportinstanz des Transportgateways zur Transportinstanz des mobilen Systems übertragen werden, als Kopien im passiven Transportgateway an den Migrationsagenten ausgeliefert. Der Migrationsagent des passiven Transportgateways erhält somit die Nutzdaten, ohne daß eine gesonderte Übertragung vom alten Transportgateway zum neuen Transportgateway erfolgt. Indem der Migrationsagent die Sequenznummern der als Kopie an ihn ausgelieferten Nutzdatenpakete analysiert, kann er die Nutzdaten an der korrekten Position des jeweiligen Empfangs- bzw. Sendepuffers (der noch nicht aktivierten Transportinstanzen) ablegen. Um die Transportinstanzen vom alten zum neuen Transportgateway zu migrieren, müssen die implizit migrierten Pufferinhalte nicht mehr vom Migrationsagenten des alten Transportgateways zum Migrationsagenten des neuen Transportgateways mittels einer gesonderten Übertragung übermittelt werden. Lediglich noch nicht beim neuen, passiven Transportgateway verfügbare Pufferinhalte und der Protokollblock müssen durch eine gesonderte Übertragung dem neuen Transportgateway verfügbar gemacht werden. Der wesentliche Vorteil der impliziten Migration ist darin zu sehen, daß für die implizite Migration von Pufferinhalten keine zusätzlichen Übertragungsressourcen erforderlich sind. Hinsichtlich der notwendigen Übertragungsressourcen stellt die implizite Migration somit geringere Anforderungen als die explizite Migration.

Die implizite Migration kann nur während der Zeiträume eingesetzt werden, während der die M-Transportinstanz Nutzdaten an das mobile System sendet. Findet keine Transportkommunikation statt, können keine Kopien der Transportprotokolldateneinheiten an den Migrationsagenten des passiven Transportgateways ausgeliefert werden und kann dieser somit auch nicht die Pufferinhalte der M-Transportinstanz rekonstruieren. Darüber hinaus können Pufferinhalte der F-Transportinstanz des Transportgateways nicht implizit migriert werden, da die zugehörigen TCP-Pakete das passive Transportgateway nicht passieren. Bei der impliziten Migration kann also nur ein Anteil der Pufferinhalte ohne gesonderte Übertragung beim

passiven Transportgateway verfügbar gemacht werden, für den anderen Anteil ist weiterhin ein gesonderte Übertragung notwendig.

4.4.3 Migration mehrerer Transportverbindungen

Betreibt ein mobiles System zum Migrationszeitpunkt mehrere indirekte Transportverbindungen gleichzeitig, so ist eine Strategie erforderlich, in welcher Reihenfolge die Statusinformation dieser Transportverbindungen vom aktiven auf das jeweils zugehörige passive Transportgateway migriert werden.

Für die Migration mehrerer Verbindungen bieten sich die folgenden zwei Alternativen an, die sich hinsichtlich der für die Migration einer Verbindung notwendigen Zeitdauer unterscheiden:

- Sequentielle Übertragung der Statusinformation mehrerer Verbindungen
  Bei der sequentiellen Migration werden erst die beiden Transportinstanzen einer indirekten Verbindung vollständig zum neuen Transportgateway migriert und anschließend wird mit der Migration der Transportinstanzen einer anderen indirekten Transportverbindung begonnen.

- Parallele Übertragung der Statusinformation mehrerer Verbindungen
  Bei der parallelen Übertragung wird beispielsweise mittels einer Round-Robin-Strategie eine indirekte Transportverbindung ausgewählt und aus den zugehörigen Transportinstanzen ein Teil der Statusinformation migriert. Obwohl diese Instanzen ggf. noch nicht vollständig migriert sind, wird anschließend Statusinformation einer anderen indirekten Transporverbindung migriert.

Hinsichtlich der Gesamtdauer, d.h. der für die Migration aller involvierten Transportinstanzen notwendigen Zeit, unterscheiden sich diese beiden Strategien nicht. Betrachtet man aber die für die Migration der Transportinstanz *einer* Verbindung notwendige Zeitdauer, so ergeben sich signifikante Unterschiede. Bei der sequentiellen Übertragung vergeht vom Start der Migration bis zum Ende der Migration der Transportinstanzen einer indirekten Transportverbindung weniger Zeit als bei der parallelen Übertragung, da während der Migration der Instanzen keine Statusinformation anderer Transportinstanzen übertragen wird.

Im Kontext der beschriebenen Nebenläufigkeit der Kommunikation auf der Transportschicht und der Übertragung der Statusinformation zum passiven Transportgateway ist die sequentielle Migration der Transportinstanzen mehrerer Transportverbindungen zu favorisieren. Da wie beschrieben die sequentielle Strategie für eine einzelne Transportverbindung eine kürzere Migrationsdauer zur Folge hat, sind Statusänderungen während der Migration weniger wahrscheinlich als bei der eine längere Migration bedingenden parallelen Strategie. Aus dem genannten Grund kommt die sequentielle Strategie zum Einsatz.

4.4.4 Unvollständige Migration wegen vorzeitiger Subnetzwechsel

Im folgenden seien aufeinanderfolgende Wechsel eines mobilen Systems von Subnetz A zu Subnetz B und ein anschließender erneuter Subnetzwechsel angenommen. Für die indirekte Transportverbindung des mobilen Systems fungiert das Transportgateway in Subnetz A

als aktives Transportgateway. Nachdem das mobile System in das Subnetz B gewechselt ist, wird mit der Migration der Transportinstanzen vom Transportgateway in Subnetz A auf das Transportgateway in Subnetz B begonnen. Bevor die Migration der Transportinstanzen abgeschlossen ist, wechselt das mobile System erneut das Subnetz. Es stellt sich somit die Frage, wie hinsichtlich der nicht vollständig beendeten Migration zu verfahren ist. Die sinnvollerweise einzusetzende Strategie ist davon abhängig, ob der erneute Wechsel zurück in Subnetz A oder in ein anderes Subnetz C erfolgt.

Wechselt das mobile System zurück in das Subnetz A, in dem es vor dem Wechsel in Subnetz B angemeldet war, sind abgesehen vom Löschen der bereits zum Transportgateway in Subnetz B migrierten Statusinformationen keine weiteren Aktionen erforderlich. Von der globalen Mobilitätsunterstützung in der Netzwerkschicht sind für das mobile System bestimmte Pakete nicht mehr in das Subnetz B, sondern in Subnetz A zu routen.

Erfolgt der vorzeitige Wechsel des mobilen Systems hingegen zu Subnetz C, so ergibt sich eine grundsätzlich andere Situation. Es bieten sich zwei verschiedene Lösungsansätze an. Eine Möglichkeit wäre es, den Teil der bereits zu dem passiven Transportgateway in Subnetz B migrierten Statusinformation in einem nachfolgenden Schritt weiter zu dem Transportgateway in Subnetz C zu migrieren und den dann noch fehlenden Teil vom Transportgateway in Subnetz A zum Transportgateway in Subnetz C zu übertragen. Wechselt das mobile System vor dem Abschluß der Migration mehrfach in ein anderes Subnetz, so sind die jeweiligen, in den Subnetzen lokalisierten Transportgateways alle in die Migration involviert, da sie jeweils einen Teil der zu migrierenden Statusinformationen gespeichert haben. Aufgrund der über die Transportgateways verteilten Statusinformation ist dieser Ansatz aufwendig zu realisieren. Darüber hinaus sind spezielle Mechanismen erforderlich, damit keine Statusinformation verloren geht.

Als Alternativmöglichkeit kann im Falle eines überlappenden Subnetzwechsels des mobilen Systems die Migration der Statusinformation von vorne begonnen werden, d.h. erneut beim aktiven Transportgateway in Subnetz A gestartet werden und die Statuinformation direkt zum Transportgateway in Subnetz C migriert werden. In diesem Fall wird die bereits teilweise auf dem vorherigen passiven Transportgateway in Subnetz B verfügbare Statusinformation gelöscht.

Die zum Subnetz B migrierte Statusinformation nicht zu verwerfen und von Subnetz B zu Subnetz C zu migrieren würde Sinn machen, falls die Migration von Subnetz B zu Subnetz C (Variante A) schneller ist als die Migration von Subnetz A zu Subnetz C (Variante B). Inwieweit Variante A schneller als Variante B ist, hängt unter anderem von den Routen, verfügbaren Bandbreiten und der Netzwerkauslastung zwischen den involvierten Transportgateways ab. Eine allgemeingültige Aussage, inwieweit Variante A bzw. Variante B zu bevorzugen ist, kann nicht gemacht werden. Aus diesem Grund erscheint es fragwürdig, die höhere Komplexität für Variante B in Kauf zu nehmen. Im Rahmen der vorliegenden Arbeit wird Variante A verfolgt, die im Falle eines vorzeitigen Subnetzwechsel die bereits migrierte Statusinformation verwirft, und einen Neustart der Migration vom alten, aktiven Transportgateway zum neuen, passiven Transportgateway im neuen Subnetz vornimmt.

4.5 Integration des OMIT-Konzeptes in Mobile IP

Die bisherigen Ausführungen beschränkten sich auf die Konzepte, die für eine effiziente Migrationsunterstützung für indirekte Transportverbindungen eingesetzt werden können. Von

einem konkreten Verfahren für die globale Mobilitätsunterstützung in der Netzwerkschicht wurde abstrahiert. Da das vorgestellte OMIT-Konzept einige spezielle Anforderungen an die die Mobilität unterstützende Netzwerkschicht stellt, sind diese hier nochmals zusammenfassend aufgeführt:

- Routing immer über das aktive Transportgateway,
- Routing auch über das passive Transportgateway (wegen impliziter Migration),
- Routing in das alte Subnetz trotz eines Subnetzwechsels und
- Forwarding der Pakete in das aktuelle Subnetz.

Da sich Mobile IP im Internet inzwischen als das Protokoll der Wahl für die globale Mobilitätsunterstützung herauskristallisiert hat, ist es wünschenswert, den indirekten Transportansatz zusammen mit Mobile IP zu betreiben. Um dieses Ziel zu erreichen, muß betrachtet werden, inwieweit sich die oben aufgeführten Anforderungen mit Mobile IP realisieren lassen bzw. inwieweit Erweiterungen oder gar Modifikationen bestehender Mobile IP Funktionalitäten notwendig sind.

Die Ausführungen beschränken sich darauf, wie Mobile IP modifiziert werden muß, um den indirekten Transportansatz einsetzen zu können, und beschreiben, wie sich die Idee des Fast Forwardings in Mobile IP umsetzen läßt. Die innerhalb eines Transportgateways erforderlichen Komponenten und ihre Interaktionen im Falle einer Puffermigration wurden bereits in Kapitel 4.3 diskutiert.

4.5.1 Positionierung des Transportgateways

Das Transportgateway muß auf einem Zwischensystem realisiert werden, über das an das mobile System adressierte Pakete garantiert geroutet werden. Darüber hinaus sollte die Paketumlaufzeit zwischen Transportgateway und dem mobilen System kurz sein, um die Vorteile des indirekten Ansatzes nutzen zu können. Potentielle Kandidaten für die Implementierung des Transportgateways sind der Home Agent und der Foreign Agent von Mobile IP.

Das Transportgateway auf dem Home Agent zu realisieren ist nicht sinnvoll, da die Entfernung zwischen dem Home Agent und dem mobilen System unter Umständen groß werden kann und sich somit für die über dieser Teilstrecke operierenden Transportverbindungen keine kurzen Paketumlaufzeiten realisieren lassen. Weiterhin werden Pakete auch nur dann über den Home Agent geroutet, falls die Routen-Optimierungsstrategie von Mobile IP [PJ00] nicht zum Einsatz kommt. Der Home Agent kommt auch deshalb nicht als Transportgateway in Frage, da vom mobilen System gesendete Pakete nicht über den Home Agent geroutet werden. Die Realisierung des Transportgateways auf dem Home Agent ist aus den genannten Gründen nicht praktikabel und wird deshalb nicht weiter verfolgt.

Kommt der *Colocated-Modus* von Mobile IP zum Einsatz, so werden für das mobile System bestimmte Pakete vom Home Agent direkt zum mobilen System getunnelt. Es kann somit – abgesehen vom Home Agent – kein Zwischensystem bestimmt werden, über das an das mobile System adressierte Pakete garantiert geroutet werden. Somit ist auch keines dieser Zwischensysteme dafür geeignet, als Transportgateway zu operieren. Der indirekte Transportansatz

kann daher zusammen mit der Variante von Mobile IP, die den Colocated-Modus nutzt, nicht realisiert werden. Im Rahmen dieser Arbeit wird deshalb von der Existenz eines Foreign Agent in den vom mobilen System besuchten Subnetzen ausgegangen.

Wird Mobile IP im *Foreign-Agent-Modus* eingesetzt, so kann das Transportgateway auf dem Foreign Agent implementiert werden. Auf Grund der geographischen Nähe des Foreign Agents zum aktuellen Aufenthaltsort des mobilen Systems ist eine kurze Round-Trip-Time der Verbindung zwischen dem Transportgateway und dem mobilen System sichergestellt. Darüber hinaus sorgt Mobile IP dafür, daß sowohl an das mobile System adressierte Pakete als auch von ihm gesendete Pakete immer über den Foreign Agent und das dort realisierte Transportgateway geroutet werden. Für die Mobile IP Variante mit Foreign Agent werden die für die Erfüllung der am Anfang des Kapitels aufgeführten vier Anforderungen notwendigen Erweiterungen und Modifikationen im folgenden Unterkapitel beschrieben.

4.5.2 Integration des Fast-Forwarding-Konzeptes

Hinsichtlich der Migrationsunterstützung können 3 Phasen unterschieden werden, die im folgenden jeweils an Abbildungen erläutert werden. Durchgezogene Linien stellen die Kommunikation zum mobilen System dar, gepunktete Linien die Kommunikation vom mobilen System zum jeweiligen Festnetzrechner. Die Tunnel zwischen dem Home Agent und dem jeweiligen Foreign Agent sind grau dargestellt. Sowohl für die normalen als auch für die getunnelten IP-Pakete sind Quell- und Zieladresse dieser Pakete in die Abbildungen mit aufgenommen. Der Festnetzrechner als Kommunikationspartner des mobilen Systems ist nicht in die Abbildungen mit aufgenommen, da er für die Beschreibung der Vorgänge keine Rolle spielt.

Abb. 4.20 zeigt die initiale Situation, bei der das mobile System noch nicht in ein anderes Subnetz gewechselt ist. Für das mobile System bestimmte Pakete werden zum Home Agent übertragen und von dort durch den Tunnel zum Foreign Agent gesendet. Die F-Transportinstanz und die M-Transportinstanz übernehmen die jeweilige Transportprotokollverarbeitung auf dem Transportgateway. Abgesehen von der Implementierung der beiden Transportinstanzen unterscheidet sich dieses Szenario nicht von einer standardmäßigen Anbindung eines mobilen Teilnehmers mittels Mobile IP.

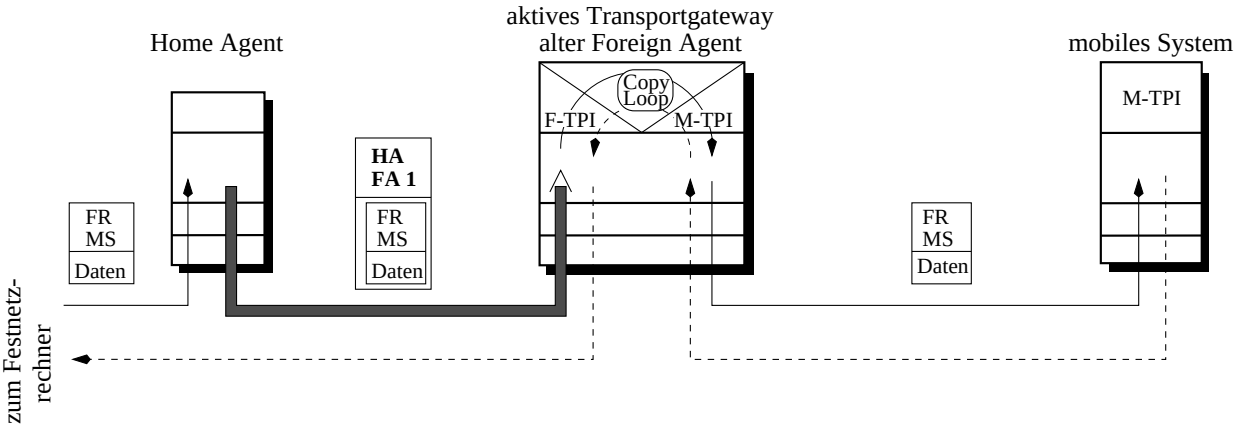


Abbildung 4.20: Phase 1 der Migration

Abb. 4.21 zeigt das Szenario, nachdem das mobile System in ein anderes Subnetz gewechselt ist. Nach dem Subnetzwechsel registriert sich das mobile System bei dem neuen Foreign

Agent. Dieser leitet allerdings die Registrierung nicht wie standardmäßig in RFC 2002 spezifiziert an den Home Agent weiter. Stattdessen verwendet er das in Kapitel 4.5.2.1 im Detail beschriebene Fast-Forwarding-Protokoll, um zwischen dem alten und dem neuen Foreign Agent einen bidirektionalen *Fast-Forwarding-Tunnel* aufzubauen. Nachdem der Tunnel aufgebaut ist, wird eine erneute Registrierung des alten Foreign Agent beim Home Agent vorgenommen. Sie dient dazu, die Registrierung beim Home Agent aufzufrischen und zu verhindern, daß wegen einer abgelaufenen Lebensdauer der Registrierung die Mobilitätsunterstützung für das mobile System beendet wird. Für das mobile System bestimmte Pakete werden auch nach dem Subnetzwechsel zum alten Foreign Agent und dem dort lokalisierten aktiven Transportgateway geroutet. Durch den Fast-Forwarding-Tunnel gelangen sowohl für das mobile System bestimmte als auch von diesem gesendete Pakete zu der aktiven F-Transportinstanz bzw. M-Transportinstanz auf dem aktiven Transportgateway. Darüber hinaus ist sichergestellt, daß diese Pakete auch den neuen Foreign Agent und das dort realisierte passive Transportgateway passieren. Im Fall der impliziten Migration werden die zu der M-Transportinstanz gehörenden Pakete als Kopie an die M-Transportinstanz des passiven Transportgateways übergeben, so daß diese Instanz bereits die jeweiligen Pufferinhalte lernen kann.

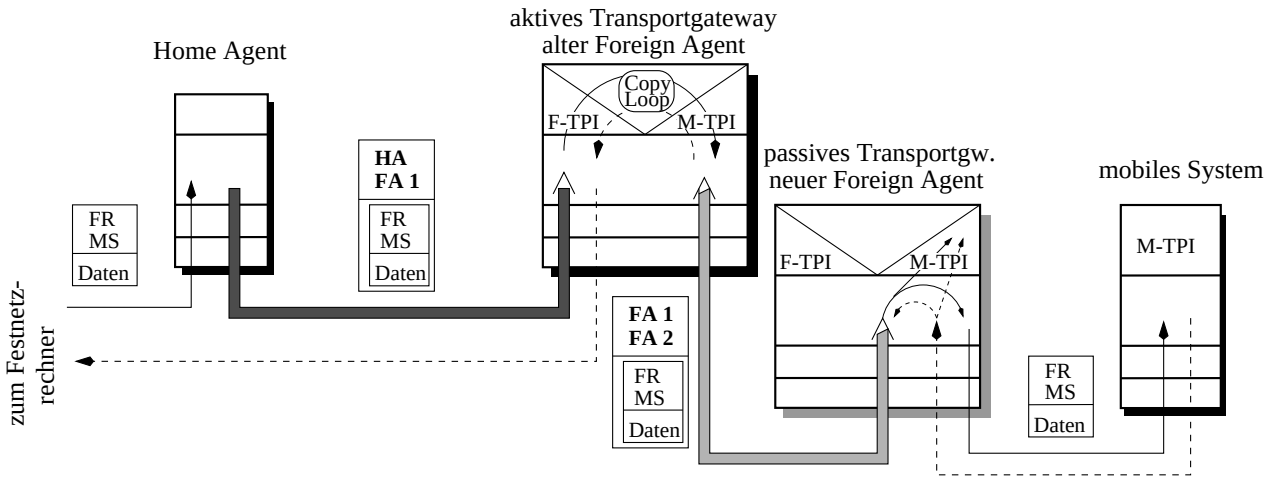


Abbildung 4.21: Phase 2 der Migration

Während das alte Transportgateway weiterhin aktiv ist und die Daten bereits über den neuen Foreign Agent an das mobile System ausgeliefert werden, können parallel die Pufferinhalte zum passiven Transportgateway migriert werden. Hierzu werden die in Abschnitt 4.4.2 beschriebenen Migrationsstrategien eingesetzt. Sobald auf dem aktiven und dem passiven Transportgateway identische Kopien aller Pufferinhalte verfügbar sind, werden die Transportverbindungen eingefroren, die Protokollkontrollblöcke übertragen, das aktive Transportgateway deaktiviert und das passive Transportgateway aktiviert.

In Abb. 4.22 ist die Situation dargestellt, nachdem das Transportgateway auf dem neuen Foreign Agent aktiviert wurde. Darüber hinaus hat sich der neue Foreign Agent direkt beim Home Agent registriert. Als unmittelbare Folge davon wird der Tunnel zwischen dem Home Agent und dem alten Foreign Agent abgebaut und der Tunnel zwischen dem Home Agent und dem neuen Foreign Agent aufgebaut. Pakete, die noch im Transit zum alten Foreign Agent sind, werden, ohne daß sie – von den inzwischen deaktivierten – Transportinstanzen bearbeitet werden, durch den Fast-Forwarding-Tunnel an den neuen Foreign Agent gesendet und dort in der F-Transportinstanz verarbeitet.

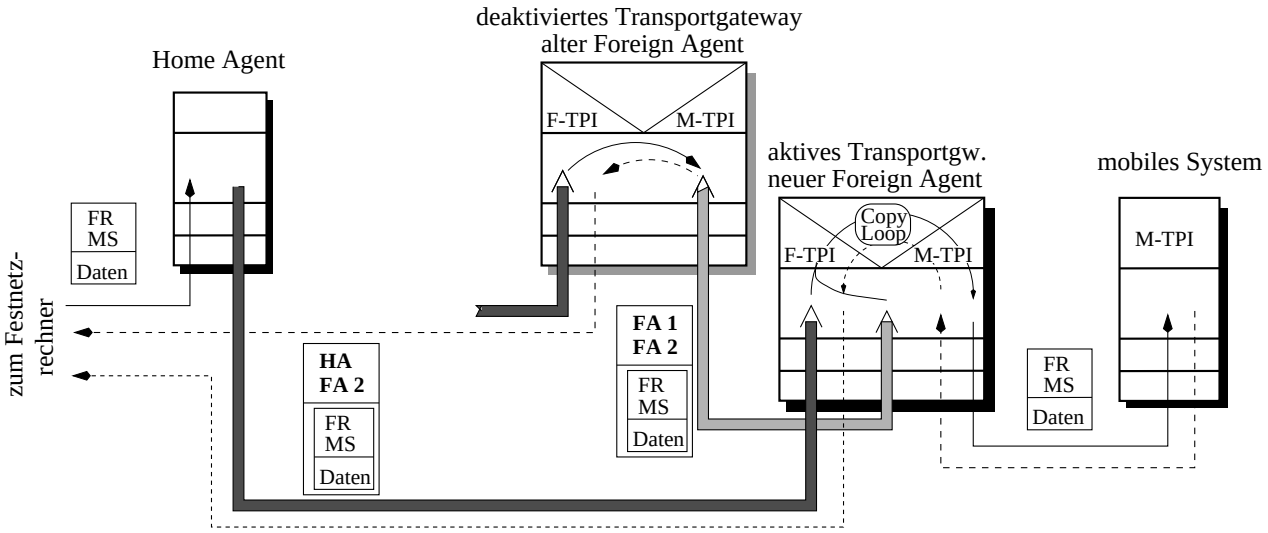


Abbildung 4.22: Phase 3 der Migration

Erreichen Pakete den Foreign Agent über den direkten Tunnel zwischen Home Agent und neuen Foreign Agent schneller als über den Fast-Forwarding-Tunnel, ergeben sich Reihenfolgevertauschungen. Das in der F-Transportinstanz realisierte Transportprotokoll TCP sendet in diesem Fall für die nicht reihenfolgetreu empfangenen Nutzdatenpakete Bestätigungs-Duplikate an den Festnetzrechner. Eine Lastreduktion gemäß der Fast-Recovery-Strategie von TCP (siehe Kapitel 2.3.1.3) seitens des Festnetzrechners ist in diesem Fall die Folge. Um die Reihenfolgevertauschung und die Lastreduktion zu vermeiden, kann die in den Unterkapiteln 4.3.1 und 4.3.2.1 beschriebene Steuerung der Zwischenpufferung dahingehend modifiziert werden, daß sie, nachdem die direkte Registrierung des neuen Foreign Agents beim Home Agent veranlaßt wurde, TCP-Pakete indirekter Transportverbindungen analysiert und ggf. zwischenpuffert. Nachdem die Pakete über den Fast-Forwarding-Tunnel empfangen wurden, werden diese zwischengepufferten Pakete weitergeleitet. TCP registriert in diesem Fall keine Reihenfolgevertauschungen.

4.5.2.1 Fast-Forwarding-Protokoll

Um den Fast-Forwarding-Tunnel zwischen dem alten und dem neuen Foreign Agent einzurichten, muß dies vom neuen an den alten Foreign Agent signalisiert werden. Abb. 4.23 zeigt die beteiligten Systeme und die zwischen diesen Systemen ausgetauschten Nachrichten. Die Registrierungsanforderung (Reg) und die Registrierungsantwort (Reply) werden wie auch bei Mobile IP zwischen dem mobilen System und dem Home Agent ausgetauscht. Um das Fast Forwarding umzusetzen, sind drei zusätzliche, im Rahmen der vorliegenden Arbeit definierte Nachrichten notwendig: *ffNotify* (Anforderung des Fast Forwardings), *ffAck* (Bestätigung bzgl. des erfolgreichen Einrichtens des Fast Forwardings) und *ffNack* (Information bzgl. des Ablehnens des Fast Forwardings). Diese drei Nachrichten werden in sogenannten *Fast-Forward-Notify-Paketen* kodiert, deren Format in Anhang A.1.2.2 dargestellt ist.

Das mobile System meldet sich nach dem Subnetzwechsel beim neuen Foreign Agent an. Die Registrierungsanforderung unterscheidet sich von der in Mobile IP spezifizierten Registrierungsanforderung dahingehend, daß vom mobilen System zusätzlich die IP-Adresse des

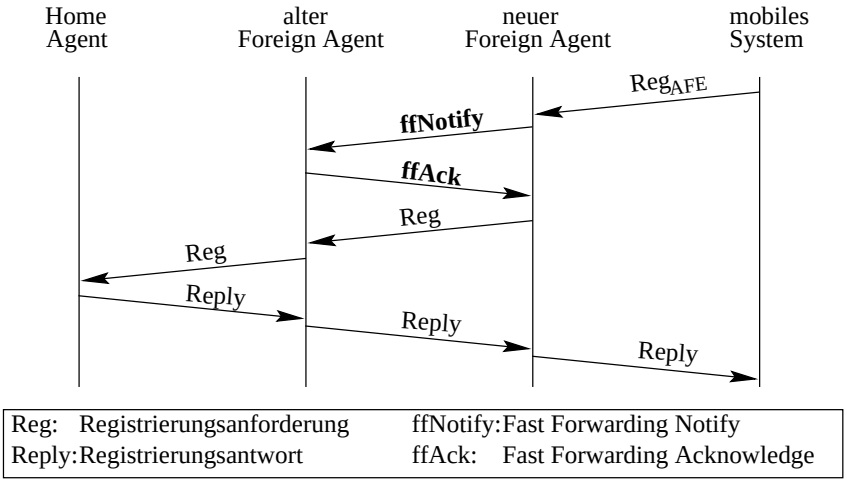


Abbildung 4.23: Registrierung beim neuen Foreign Agent (mit Fast Forwarding)

letzten Foreign Agents mit angegeben wird. Diese IP-Adresse wird in der *Alten-Foreign-Agent-Erweiterung* kodiert, die an die Mobile IP Registrierung angehängt wird und deren Format in Anhang A.1.2.1 aufgeführt ist. Anhand dieser zusätzlichen Adresse erkennt der neue Foreign Agent den Wunsch des mobilen Systems nach Anbindung mittels der Fast-Forwarding-Strategie. In Abb. 4.23 wird die Registrierung mit angehängter Alter-Foreign-Agent-Erweiterung mit Reg_{AFE} bezeichnet.

Kann der neue Foreign Agent das Forwarding unterstützen, sendet er eine *Fast-Forward-Notify-Nachricht* (ffNotify) an den alten Foreign Agent und fordert diesen damit auf, das Fast Forwarding für das jeweilige mobile System zu aktivieren. Stehen die für das Fast Forwarding notwendigen Ressourcen beim alten Foreign Agent zur Verfügung, wird die lokale Unterstützung des mobilen Systems beendet und der Fast-Forwarding-Tunnel zum neuen Foreign Agent geöffnet. Das mobile System ist nach Einrichtung des Fast-Forwarding-Tunnels wieder erreichbar. Mittels einer *Fast-Forward-Acknowledge-Nachricht* (ffAck) wird dem neuen Foreign Agent die Einrichtung des Fast Forwardings beim alten Foreign Agent bestätigt.

Die Einrichtung des Fast-Forwarding-Tunnels ist allerdings nicht ausreichend für eine dauerhafte Anbindung des mobilen Systems. Empfangen das mobile System, der alte und der neue Foreign Agent bzw. der Home Agent innerhalb der Lebensdauer einer Registrierung keine vom Home Agent ausgesendeten Registrierungsantworten, wird die Mobilitätsunterstützung für das zugehörige mobile System eingestellt. Aus diesem Grund muß eine periodische Reregistrierung auch im Falle der Verwendung des Fast-Forwarding-Konzeptes vorgenommen werden. Nachdem der neue Foreign Agent die Fast-Forward-Acknowledge-Nachricht erhalten hat, sendet er die Registrierungsanforderung (Reg) des mobilen Systems an den alten Foreign Agent. Dieser wiederum leitet die Registrierung an den Home Agent weiter, der daraufhin den den Ablauf der Registrierung überwachenden Timer neu initialisiert. Die Registrierungsantwort (Reply) wird über den alten Foreign Agent und den neuen Foreign Agent zum mobilen System geschickt, so daß alle drei Systeme ihre Timer neu initialisieren können. Somit kann das Ablaufen der Timer und ein Beenden der Unterstützung für das mobile System verhindert werden.

Kann der alte Foreign Agent das Fast Forwarding nicht unterstützen, ergibt sich die in Abb. 4.24 dargestellte Situation. Nachdem der neue Foreign Agent vom alten Foreign Agent

mittels einer *Fast-Forward-Negative-Acknowledge-Nachricht* (ffNack) darüber informiert wurde, daß der alte Foreign Agent das Fast Forwarding nicht unterstützt, registriert sich der neue Foreign Agent direkt beim Home Agent. Der neue Foreign Agent registriert sich auch dann direkt bei Home Agent, falls er selbst kein Fast Forwarding bietet. Da in beiden Fällen kein Fast Forwarding möglich ist, kann die Migration der Transportinstanzen nicht nebenläufig erfolgen. Es muß stattdessen eine Migration mit Einfrieren vorgenommen werden.

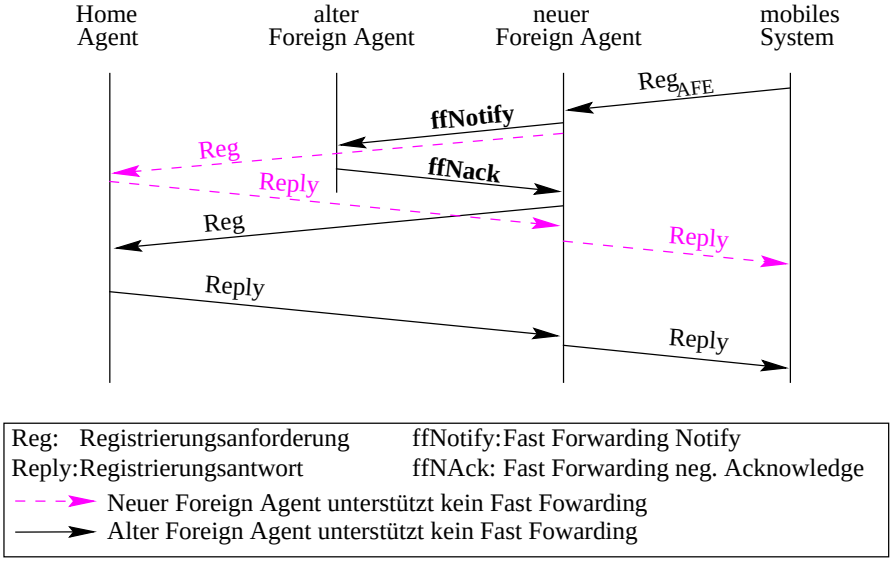


Abbildung 4.24: Registrierung beim neuen Foreign Agent (Fast Forwarding abgelehnt)

Zustandsübergangsdiagramm für den Foreign Agent

Für jedes unterstützte mobile System muß im Foreign Agent der aktuelle Zustand gespeichert werden. Abb. 4.25 zeigt sowohl das Zustandsübergangsdiagramm mit den verschiedenen Zuständen als auch die für die Zustandsübergänge verantwortlichen Eingabeereignisse und die Reaktionen in der Notation *Ereignis*; *Reaktion*.

Im Zustand „Init“ befindet sich der Automat, falls das mobile System aktuell nicht beim Foreign Agent registriert ist. Der Zustand „Pending“ reflektiert, daß ein mobiles System derzeit nicht beim Foreign Agent registriert ist, eine Registrierungsanforderung empfangen und an den Home Agent weitergeleitet wurde, aber noch keine Antwort vom Home Agent empfangen wurde. Im Zustand „Confirmed“ hat der Foreign Agent eine Mobilitätsunterstützung für das mobile System eingerichtet. An das mobile System adressierte IP-Pakete werden lokal ausgeliefert. Im Zustand „Pending Rereg“ hat der Foreign Agent ebenfalls eine lokale Mobilitätsunterstützung eingerichtet. Darüber hinaus wartet er auf eine Registrierungsantwort vom Home Agent für die periodisch gesendete Registrierungsanforderung. Die genannten Zustände sind auch bei Mobile IP ohne Fast Forwarding vorhanden.

Bei Mobile IP mit Fast Forwarding werden zusätzlich die grau unterlegten Zustände erforderlich. Im Zustand „Pending Notify“ befindet sich ein Foreign Agent, der beim alten, vorherigen Foreign Agent das Fast Forwarding angefordert hat, aber noch keine Antwort bezüglich des Erfolges dieser Anforderung erhalten hat. Im Zustand „Fast Forward“ ist der Foreign Agent in die Mobilitätsunterstützung des mobilen Systems involviert. Er leitet an das mobile System adressierte Pakete in den Fast-Forwarding-Tunnel weiter zum nächsten bzw.

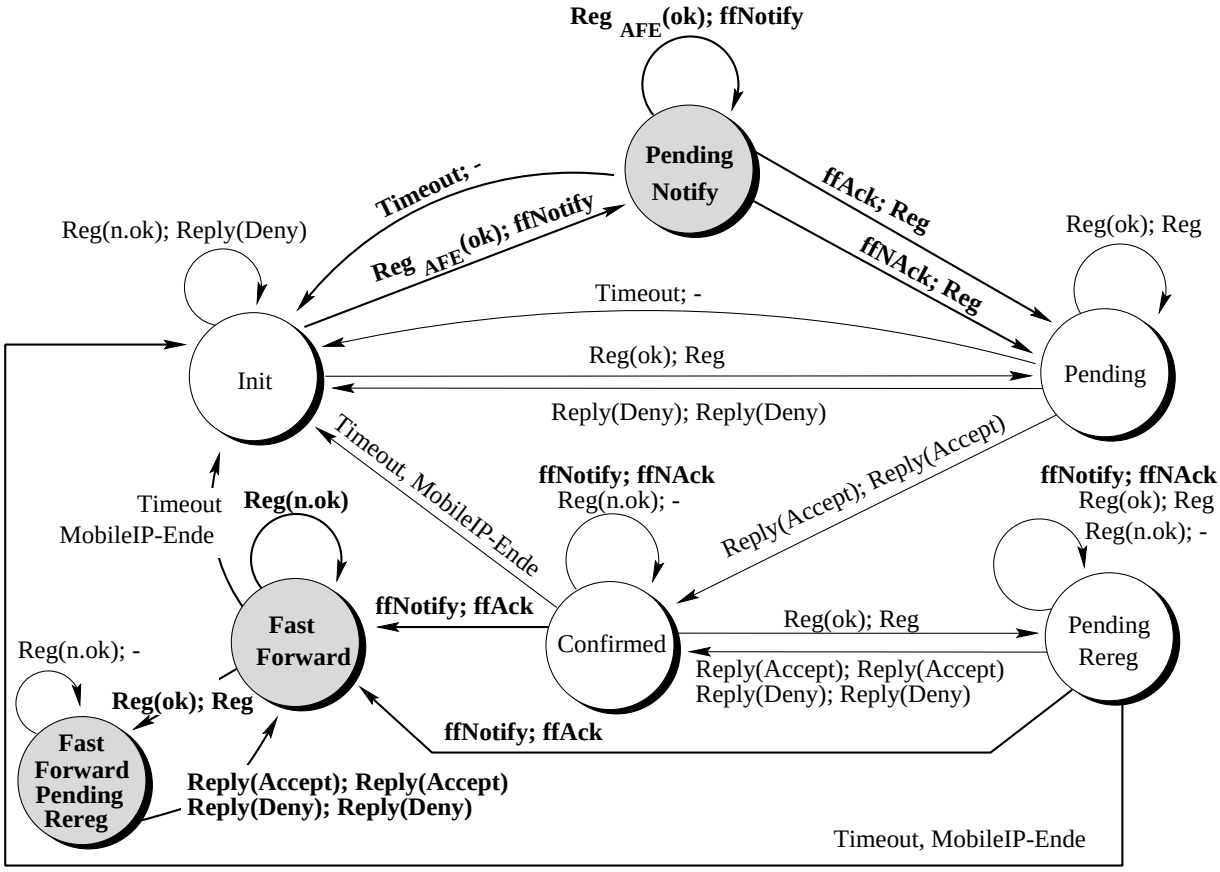


Abbildung 4.25: Zustandsübergangsdiagramm des Foreign Agents

vorherigen Agent. Auch im Zustand „Fast Forwarding Pending Rereg“ werden Pakete in den Tunnel weitergeleitet. Darüber hinaus wartet der Foreign Agent in diesem Zustand auf eine Registrierungsantwort für die periodisch gesendete Registrierungsanforderung.

Reg(ok), Reg(n.ok), Reply(Accept), Reply(Deny) und Timeout sind Ereignisse, die auch ohne Fast Forwarding eintreten. Im Fall von Reg(ok) hat der Foreign Agent eine Registrierungsanforderung empfangen und akzeptiert, im Fall von Reg(n.ok) empfangen und abgelehnt. Reply(Accept) bzw. Reply(Deny) bedeuten den Empfang einer Registrierungsantwort mit einer akzeptierten bzw. abgelehnten Registrierung. Das Ereignis Timeout tritt bei Ablaufen der Lebensdauer einer Registrierung ein. Die Bedeutung der durch den Empfang der jeweiligen Nachrichten bedingten Eingabeereignisse ffNotify, ffAck und ffNack ist bereits zu Beginn dieses Unterkapitels beschrieben.

Bei der folgenden Beschreibung der Zustandsübergänge liegt der Fokus auf den Übergängen, die durch die Fast-Forwarding-Erweiterung für Mobile IP bedingt sind. Vorgänge, die in gleicher Form auch bei Mobile IP ohne Fast Forwarding auftreten, werden nicht diskutiert. Eine Beschreibung dieser Abläufe ist in Kapitel 2.2 bzw. im Detail in [Per98a] zu finden.

Empfängt ein Foreign Agent eine Registrierungsanforderung mit Alter-Foreign-Agent-Erweiterung (Reg_{AFE}) und kann er diese Anforderung erfüllen, fordert er mittels einer ffNotify-Nachricht beim alten Foreign Agent das Fast Forwarding an und wechselt in den Zustand „Pending Notify“. Von dort wechselt er in den Zustand „Pending“, sobald er vom alten Foreign Agent eine ffAck- oder ffNAck-Nachricht erhält. Im Falle der ffAck-Nachricht wurde der

Fast-Forwarding-Tunnel eingerichtet. Die Registrierung wird daher zum alten Foreign Agent weitergeleitet (siehe Abb. 4.23). Empfängt er eine ffNack-Nachricht, wird das Fast Forwarding nicht unterstützt. Daher erfolgt eine direkte Registrierung beim Home Agent (siehe Abb. 4.24). Geht eine ffNotify- oder ffAck- oder ffNack-Nachricht verloren, sendet das mobile System nach einer gewissen Zeit erneut eine Reg_{AFE}-Nachricht. Der Foreign Agent bleibt in diesem Fall im Zustand „Pending Notify“ und fordert mittels einer ffNotify-Nachricht erneut beim alten Foreign Agent das Fast Forwarding an.

Ein direkter Übergang vom Zustand „Init“ in den Zustand „Pending“ erfolgt, falls eine Registrierungsanforderung (*Reg*) ohne Alte-Foreign-Agent-Erweiterung empfangen wird. Kann der Foreign Agent das mobile System unterstützen, wird die Registrierung an den Home Agent weitergeleitet. Aus dem Zustand „Pending“ wechselt der Foreign Agent in den Zustand „Confirmed“, sobald er mittels einer Reply(Accept)-Nachricht über den Erfolg einer Registrierung informiert wird. Diese Reply-Nachricht wird an das mobile System weitergeleitet.

In den Zuständen „Confirmed“ und „Pending Rereg“ ist die lokale Mobilitätsunterstützung von Mobile IP für das mobile System eingerichtet. Empfängt der Foreign Agent in einem dieser beiden Zustände eine ffNotify-Nachricht und kann er das Fast-Forwarding unterstützen, richtet er den Fast-Forwarding-Tunnel ein und sendet eine ffAck-Nachricht an den Foreign Agent, der das Fast Forwarding angefordert hat. Zusätzlich erfolgt ein Wechsel in den Zustand „Fast Forward“. Kann das Fast Forwarding nicht unterstützt werden, wird eine ffNack-Nachricht gesendet und kein Zustandswechsel vorgenommen. Nach Empfang einer Registrierungsanforderung, die der Foreign Agent erfüllen kann, wechselt der Foreign Agent aus dem Zustand „Fast Forward“ in den Zustand „Fast Forwarding Pending Rereg“ und leitet die Registrierungsanforderung an den vorangehenden Agent weiter. Sobald die zugehörige Reply-Nachricht beim Foreign Agent eintrifft, erfolgt ein Übergang zurück in den Zustand „Fast Forwarding“, und die Reply-Nachricht wird weitergeleitet.

4.5.2.2 Fast Forwarding und aufeinanderfolgende Subnetzwechsel

Wechselt ein mobiles System in ein anderes Subnetz nachdem das Forwarding zwischen dem alten und dem neuen Foreign Agent aktiviert wurde, aber bevor der neue Foreign Agent sich direkt beim Home Agent registriert hat, so stellt sich die Frage, zwischen welchen Foreign Agents der Fast-Forwarding-Tunnel aufgebaut wird. Abb. 4.26 zeigt ein derartiges Szenario. Das mobile System war beim 2.FA angemeldet und wechselt nun, bevor ein direkter Tunnel zwischen Home Agent und 2.FA etabliert wird, zum 3.FA. Im dargestellten Szenario hat das mobile System zwei Transportverbindungen geöffnet und mit der Migration der zu diesen Verbindungen gehörigen Statusinformation bereits begonnen. Die Transportinstanzen der ersten Verbindung wurden bereits zum Transportgateway auf dem 2.FA migriert, für die zweite Verbindung fungiert hingegen der 1.FA noch als Transportgateway.

Im beschriebenen Szenario stellt sich die Frage, zwischen welchen Foreign Agents der Fast-Forwarding-Tunnel nach dem Wechsel zum 3.FA eingerichtet wird. In Abb. 4.26 ist der Tunnel zwischen dem letzten Foreign Agent, d.h. dem 2.FA, und dem 3.FA eingerichtet. Wird diese Strategie verfolgt, so können sich im Fall mehrerer vorzeitiger Subnetzwechsel sogenannte *Fast-Forwarding-Tunnelketten* und darüber hinaus auch Schleifen in den Fast-Forwarding-Tunnelketten bilden.

Wird hingegen wie in Abb. 4.27 dargestellt nach jedem Subnetzwechsel ein Fast-Forwar-

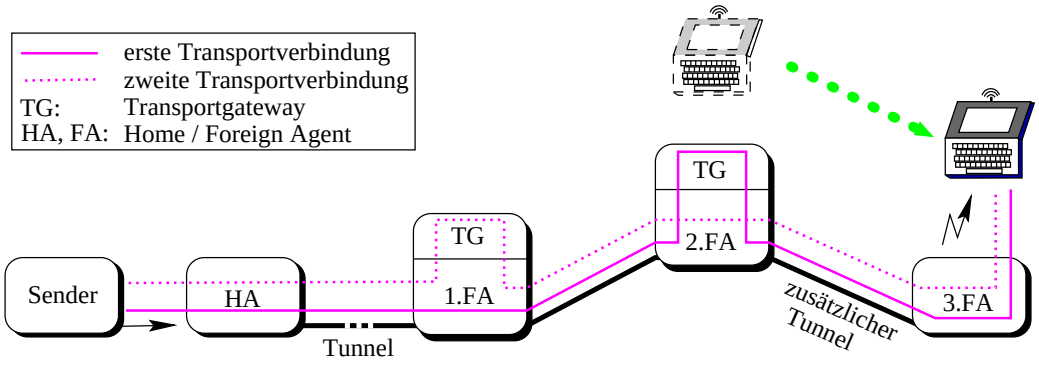


Abbildung 4.26: Fast Forwarding: Variante mit zusätzlichem Tunnel

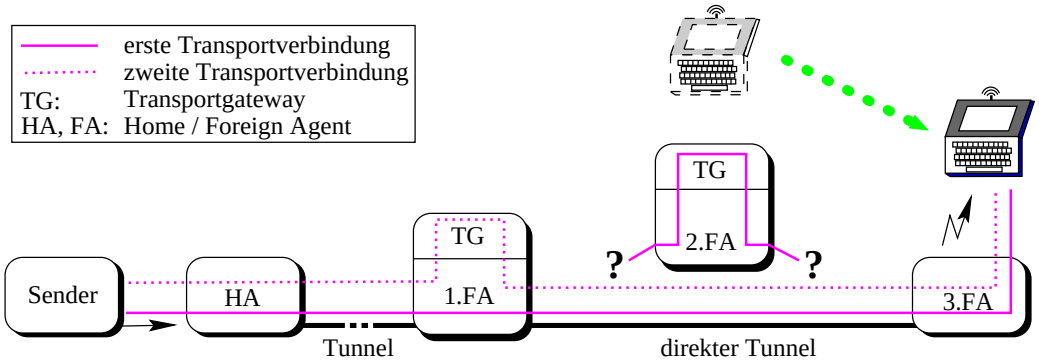


Abbildung 4.27: Fast Forwarding: Variante mit direktem Tunnel

ding-Tunnel zwischen dem 1.FA und dem neuen – in diesem Falle 3.FA – eingerichtet, so sind maximal zwei Foreign Agents involviert. Probleme hinsichtlich Fast-Forwarding-Tunnelketten und Schleifen in diesen Ketten können sich somit in diesem Fall nicht ergeben.

Betrachtet man lediglich die Konnektivität auf IP-Ebene, so erscheint der zweite Ansatz auf Grund der geringeren Komplexität als besser geeignet. Berücksichtigt man allerdings, daß auf den Foreign Agents Transportgateways realisiert sind, stellt sich die Situation anders dar. Da die Transportinstanzen der ersten Verbindung bereits zum Transportgateway auf dem 2.FA migriert und dort auch aktiviert wurden, muß sichergestellt sein, daß die Pakete weiterhin über den zweiten Foreign Agent geroutet werden. Der in Abb. 4.27 dargestellte Ansatz kann dies nicht sicherstellen. Das auf dem 2.FA realisierte Transportgateway ist abgekoppelt und kann nicht mehr als Transportgateway für die erste Verbindung genutzt werden.

Bei allen weiteren Betrachtungen wird davon ausgegangen, daß bei jedem Subnetzwechsel ein Fast-Forwarding-Tunnel zum vorherigen Foreign Agent aufgebaut wird. Das Problem sich entwickelnder Fast-Forwarding-Tunnelketten und sich bildender Schleifen muß somit adressiert werden.

4.5.2.3 Fast-Forwarding-Tunnelkette

Fast-Forwarding-Tunnelketten können sich ausbilden, falls ein mobiles System mehrmals das Subnetz wechselt und nach jedem Subnetzwechsel statt einer direkten Registrierung beim Home Agent ein Fast-Forwarding-Tunnel zwischen dem alten und dem neuen Foreign Agent eingerichtet wird. In den Datenfluß zwischen dem Home Agent und dem mobilen System sind

in diesem Falle mehrere Foreign Agents involviert. Abb. 4.28 verdeutlicht die sich ergebende Situation.

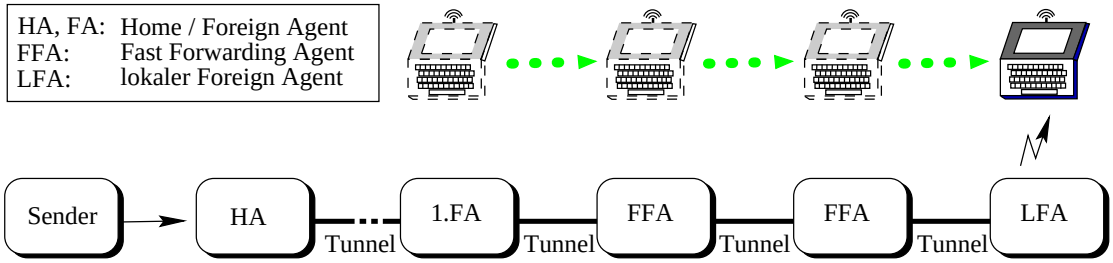


Abbildung 4.28: Fast-Forwarding-Tunnelkette

Der Foreign Agent, der die vom Home Agent in den Tunnel gesendeten Pakete empfängt wird der *1.FA* genannt. Unter einem *lokalen Foreign Agent* versteht man den Foreign Agent, bei dem das mobile System direkt angemeldet ist, d.h der Foreign Agent, der die lokale Unterstützung für das mobile System eingerichtet hat. Die zwischen dem ersten Foreign Agent und dem lokalen Foreign Agent angesiedelten Foreign Agents werden als die *Fast Forwarding Agents* (FFA) bezeichnet. Verlängert sich im Zuge eines Subnetzwechsels die Fast-Forwarding-Tunnelkette um einen Foreign Agent, so wird aus dem alten lokalen Foreign Agent ein Fast Forwarding Agent. Der neue Foreign Agent übernimmt die Rolle des lokalen Foreign Agent.

Da durch dieses Verfahren sichergestellt ist, daß alle vom mobilen System gesendeten bzw. empfangenen Pakete über den 1.FA, die Fast Forwarding Agents und den lokalen Foreign Agent gesendet werden, kann auf allen diesen Foreign Agents das Transportgateway realisiert werden.

4.5.2.4 Fast-Forwarding-Schleifen

Fast-Forwarding-Schleifen entstehen, falls ein mobiles System in ein Subnetz wechselt, in dem es zu einem früheren Zeitpunkt bereits registriert war und darüber hinaus der Foreign Agent dieses Subnetzes in die Fast-Forwarding-Tunnelkette zum mobilen System involviert ist. Ein Szenario mit einer Fast-Forwarding-Schleife ist in Abb. 4.29 dargestellt. Das mobile System war nacheinander beim 2.FA, beim 3.FA und beim 4.FA registriert und wechselt anschließend wieder zurück in das Subnetz des 2.FA. Nachdem das mobile System zum 2.FA gewechselt ist, wird ein Fast-Forwarding-Tunnel zum 4.FA aufgebaut. Es bildet sich somit eine Schleife.

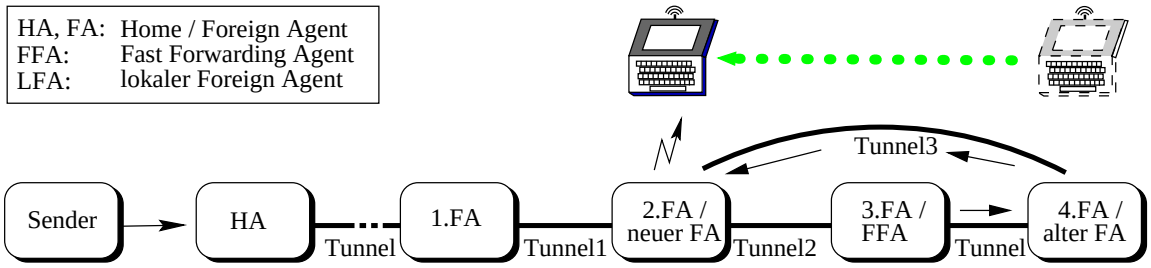


Abbildung 4.29: Fast-Forwarding-Schleife

Beim 2.FA kann zwar festgestellt werden, daß sich eine Schleife gebildet hat, sie kann aber nicht sofort aufgelöst werden, da der 3.FA bzw. der 4.FA möglicherweise für indirekte

Transportverbindungen des mobilen Systems als Transportgateway fungieren. Im Falle einer sofortigen Schleifenauflösung wären die Transportgateways abgekoppelt. Wegen dieser Problematik wird, unabhängig davon ob sich durch den Aufbau eines Fast-Forwarding-Tunnels eine Schleife ergibt oder nicht, dieser Tunnel eingerichtet. Die Auflösung einer Schleife kann nur dann erfolgen, falls sichergestellt ist, daß kein Foreign Agent innerhalb der Schleife für das mobile System als Transportgateway fungiert. Durch eine Migration kann ggf. ein Transportgateway auf einen Foreign Agent außerhalb der Schleife verlagert werden. Verfahren zur Schleifenerkennung und Schleifenauflösung sind in Kapitel 4.5.2.5 beschrieben.

Im Falle sich bildender Schleifen muß dem Routing besondere Aufmerksamkeit gewidmet werden. Im in Abb. 4.29 skizzierten Szenario passieren an das mobile System adressierte Pakete zweimal den 2.FA. Pakete, die vom 1.FA zum 2.FA durch den Fast-Forwarding-Tunnel gesendet werden, müssen durch einen weiteren Fast-Forwarding-Tunnel zum 3.FA übertragen werden. Pakete, die vom 4.FA zum 2.FA gesendet werden, müssen hingegen über das lokale Subnetz zum mobilen System ausgeliefert werden. Im 2.FA kann somit für Pakete, die an das mobile System adressiert sind, die Routingentscheidung nicht alleine auf Basis der Zieladresse des IP-Pakets getroffen werden. Für die Routingentscheidung muß mit berücksichtigt werden, über welches Interface bzw. welchen Tunnel ein Paket vom 2.FA empfangen wurde. Unterstützung hierfür ist beispielsweise in das Betriebssystem Linux bereits integriert. Unter der Annahme, daß der Laptop im in Abb. 4.29 skizzierten Szenario die IP-Adresse 134.169.34.210 hat, zeigt Abb. 4.30 die Routingtabelle für den 2.FA. In Abhängigkeit davon, über welches Tunnel-Interface der 2.FA ein an den Laptop adressiertes Paket empfängt, sendet er es entweder in das Interface Tunnel2 oder über das wireless Interface auf den Funkkanal zum Laptop.

Routing-Präfix	Empfangs-Interface	Sende-Interface
134.169.34.210/32	Tunnel1	Tunnel2
134.169.34.210/32	Tunnel3	wireless Interface
⋮	⋮	⋮

Abbildung 4.30: Routingtabelle des 2.FA

Um das Routing durch die Fast-Forwarding-Tunnelkette zu realisieren, ist in jedem Foreign Agent dieser Kette für ein mobiles System, zu dem die Pakete durch diese Kette geroutet werden, mindestens ein Eintrag in der Routingtabelle erforderlich. Diese zusätzlichen Tabelleneinträge stellen aber kein signifikantes Problem dar, da sie nicht auf zentral im Internet angesiedelten Routern, die ohnehin schon große Routingtabellen haben, erfolgen und darüber hinaus wegen der möglichen Auflösung von Fast-Forwarding-Ketten nicht von Dauer sind.

4.5.2.5 Schleifenerkennung

Bevor eine Schleife aufgelöst werden kann, muß zunächst ihre Existenz festgestellt werden. In diesem Kontext ist zu klären, welches System überhaupt die Existenz einer Schleife erkennen kann. Ein Foreign Agent, bei dem sich ein mobiles System neu anmeldet und gemäß des Fast-Forwarding-Protokolls die Einrichtung eines Fast-Forwarding-Tunnels zwischen diesem Foreign Agent und dem alten Foreign Agent anfordert, kann durch Analyse der Routingtabellen

ermitteln, ob im Falle der Einrichtung dieses Tunnels eine Schleife entsteht. Ergibt die Analyse der Routingtabelle, daß für das mobile System bereits das Fast-Forwarding unterstützt wird, so liegt eine Schleife vor. An das mobile System adressierte Pakete passieren den Foreign Agent dann mehrfach. Allerdings kann dieser Foreign Agent nicht feststellen, ob Foreign Agents innerhalb der Schleife für Verbindungen des mobilen Systems als Transportgateway fungieren. Aus diesem Grunde kann er auch nicht die Auflösung der Schleife veranlassen.

Im Rahmen der vorliegenden Arbeit wird der Ansatz verfolgt, sowohl die Schleifenerkennung als auch die Steuerung der Schleifenauflösung auf dem mobilen System zu realisieren. Um eine Schleife erkennen zu können, muß das mobile System Kenntnis haben, welche Foreign Agents in die Fast-Forwarding-Tunnelkette involviert sind. Ist ein Foreign Agent mehrfach in eine Tunnelkette involviert, so liegt eine Schleife vor. Darüber hinaus muß das mobile System darüber informiert sein, auf welchen Foreign Agents der Fast-Forwarding-Tunnelkette Transportgateways realisiert sind. Diese Information ist notwendig, da andernfalls die Gefahr besteht, daß nach einer Schleifenauflösung das Transportgateway nicht mehr im Datenpfad liegt.

Um das mobile System über die IP-Adressen der in die Tunnelkette involvierten Foreign Agents und die IP-Adressen der Systeme, die als Transportgateway fungieren, zu informieren, wird das Mobile IP Protokoll erweitert. Registrierungsanforderungen und Registrierungsantworten von Mobile IP werden entlang der Fast-Forwarding-Tunnelkette zwischen Home Agent und dem mobilem System ausgetauscht und sind somit prädestiniert für die Übermittlung der IP-Adressen der in die Tunnelkette involvierten Foreign Agents zum mobilen System. Hierzu wird eine neue Mobile IP Extension, die sogenannte *Schleifenerkennungs-Erweiterung* (siehe Anhang A.1.2.3) eingeführt. An die vom Home Agent zum mobilen System gesendete Registrierungsantwort wird diese Schleifenerkennung-Erweiterung am Ende angefügt. Passiert eine Registrierungsantwort einen Foreign Agent, hängt dieser zusätzlich eine Schleifenerkennungs-Erweiterung an die Registrierungsantwort an. In diese trägt er die IP-Adresse des Interfaces, über das die Registrierungsantwort empfangen wurde, ein und vermerkt, ob der Foreign Agent für dieses mobile System als Transportgateway operiert. Darüber hinaus untersucht der Foreign Agent, ob eine bereits in der Mobile IP Extension der Registrierungsantwort kodierte IP-Adresse mit einer IP-Adresse eines Interfaces des Foreign Agents übereinstimmt. Wird eine Übereinstimmung festgestellt, passiert die Registrierungsantwort mindestens zum zweiten Mal den Foreign Agent. Es liegt somit eine Schleife vor. Die Existenz der Schleife wird ebenfalls in der Mobile IP Extension der Registrierungsantwort kodiert.

Empfängt das mobile System die Registrierungsantwort zuzüglich der Schleifenerkennungs-Erweiterungen, kann es anhand der in den Erweiterungen kodierten Informationen ermitteln, ob die Fast-Forwarding-Tunnelkette eine Schleife enthält und welcher Foreign Agent mit welchen Interfaces in die Schleife involviert ist. Liegt keine Schleife vor, sind keine weiteren Maßnahmen zu ergreifen. Existiert eine Schleife, wird die im folgenden beschriebene Schleifenauflösung gestartet.

4.5.2.6 Schleifenauflösung

Existiert eine Schleife, werden IP-Pakete des mobilen Systems durch eine unnötig lange Tunnelkette transportiert. Trotz dieser Ineffizienz werden an das mobile System adressierte bzw. von ihm gesendete Pakete korrekt geroutet, d.h. die Netzwerkkonnektivität des mobilen Systems bleibt trotz der Schleife erhalten.

Abb. 4.31 zeigt die Migrationssteuerung, die im mobilen System für die Erkennung und die Auflösung einer Schleife verantwortlich ist. Von Mobile IP werden die Schleifenerkennungs-Erweiterungen an die Migrationssteuerung übergeben. Ergibt die Analyse dieser Daten, daß keine Schleife vorliegt, sind keine weiteren Aktionen zu veranlassen. Liegt eine Schleife vor, sind die weiteren Aktionen davon abhängig, ob ein innerhalb der Schleife angesiedelter Foreign Agent für das mobile System als Transportgateway fungiert oder nicht.

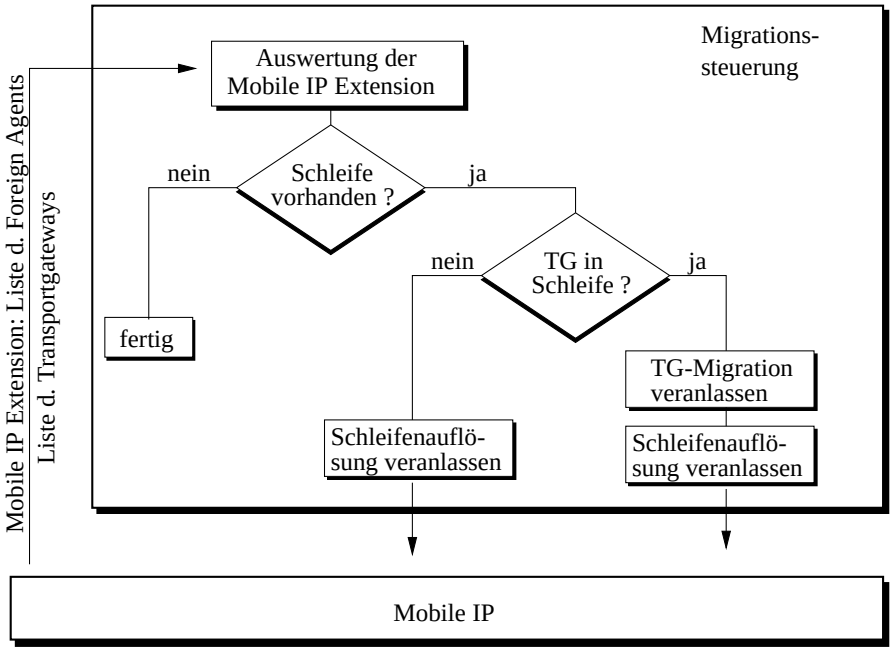


Abbildung 4.31: Migrationssteuerung im mobilen System

Kein Transportgateway in der Schleife realisiert
Ist innerhalb der Schleife kein Transportgateway angesiedelt, kann sofort eine Auflösung der Schleife veranlaßt werden. Eine Mobile IP Nachricht wird hierzu an den Foreign Agent gesandt, bei dem die Schleife aufgelöst wird. In diesem Foreign Agent wird bei Empfang der Nachricht für die Schleifenauflösung die Routingtabelle modifiziert. Soll im in Abb. 4.29 skizzierten Szenario eine Schleifenauflösung beim 2.FA erfolgen, werden die beiden in Abb. 4.30 dargestellten Einträge aus der Routingtabelle gelöscht und ein neuer Eintrag hinzugefügt. Dieser neue Eintrag sorgt dafür, daß an die Adresse 134.169.34.210 adressierte Pakete über das wireless Interface gesendet werden, d.h. direkt an den Laptop ausgeliefert werden.

Da Mobile IP einen unzuverlässigen Übertragungsdienst nutzt, ist nicht sichergestellt, daß die die Schleifenauflösung veranlassende Mobile IP Nachricht erfolgreich zum jeweiligen Foreign Agent übertragen wird. Im Falle eines Verlustes dieser Nachricht wird die Schleife nicht aufgelöst. Von der Migrationssteuerung wird deshalb nach der nächsten von Mobile IP periodisch durchgeführten Registrierung die Existenz dieser Schleife erneut festgestellt und dann ihre Auflösung wiederum durch eine Mobile IP Nachricht veranlaßt. Alternativ ist auch vorstellbar, nicht erst die nächste periodische Registrierung von Mobile IP abzuwarten, sondern nach Übertragung der Mobile IP Nachricht für die Schleifenauflösung eine erneute Mobile IP Registrierungsnachricht zu senden. In diesem Falle erhält das mobile System schneller ein

Feedback, ob die Schleife erfolgreich aufgelöst wurde und kann ggf. eine erneute Schleifenauflösung veranlassen.

Transportgateway in der Schleife realisiert
Fungiert innerhalb der Schleife ein Foreign Agent als Transportgateway, muß zunächst eine Migration vorgenommen werden. Das mobile System kennt die Fast-Forwarding-Tunnelkette und kann somit entscheiden, auf welchen Foreign Agent das Transportgateway migriert werden soll. Es selbst ist nur insofern in die Migration involviert, daß es die Migration veranlaßt und über das Ende informiert wird. Veranlaßt wird die Migration, indem an das Transportgateway-Management im alten Transportgateway die Aufforderung gesendet wird, eine Migration vorzunehmen. Das alte Transportgateway kann dieser Aufforderung entnehmen, welche Transportinstanzen zu welchem neuen Transportgateway migriert werden sollen. Welche einzelnen Schritte vom Transportgateway-Management für die Migration veranlaßt werden, ist in Kapitel 4.3.3.4 beschrieben. Sobald das mobile System über den Abschluß der Migration informiert ist, kann es die Auflösung der Schleife veranlassen. Da nach der Migration kein Transportgateway mehr in der Schleife realisiert ist, kann das zuvor beschriebene Verfahren für die Schleifenauflösung eingesetzt werden.

4.5.3 Mobiles System im Heimatsubnetz

Um den indirekten Transportansatz einsetzen zu können, müssen die Pakete auch dann über das Transportgateway geroutet werden, falls das mobile System in seinem Heimatsubnetz an das Internet angebunden ist. Es bietet sich in diesem Fall an, das Transportgateway auf dem Home Agent zu realisieren. Allerdings muß zusätzlich erzwungen werden, daß die Pakete des mobilen Systems auch im Heimatsubnetz über den Home Agent geroutet werden. Erreicht wird dies, indem abweichend von der Spezifikation von Mobile IP keine Deregistrierung im Heimatsubnetz vorgenommen wird. Somit werden die Pakete nicht direkt zu dem im Heimatsubnetz angesiedelten mobilen System geroutet, sondern über den Home Agent, der dann als Transportgateway fungieren kann.

4.6 Zusammenfassung

Um die wegen der Mobilität mobiler Endsysteme erforderlichen Migrationen von Transportinstanzen und die durch diese Migrationen bedingten Unterbrechungen zu vermeiden, wurde das OMIT-Konzept entwickelt. OMIT umfaßt einen Eingriff in das Routing, damit trotz Subnetzwechseln eines mobilen Systems die Pakete über das alte Transportgateway geroutet werden und somit keine Migration erforderlich wird. Darüber hinaus ist die nebenläufige Migration, die die durch die Migration bedingte Unterbrechung reduzieren kann, eine wesentliche Komponente von OMIT.

Zentrale Idee des Eingriffs in das Routing ist es, die globale Mobilitätsunterstützung nicht zu veranlassen, die Pakete ins neue Subnetz zu routen. Stattdessen wird das Routing in das alte Subnetz beibehalten, und zusätzlich ein sogenannter Forwarding-Tunnel zwischen dem alten und den neuen Subnetz etabliert. Wie sich diese Strategie in Mobile IP integrieren läßt und wie sich ggf. bildende Ketten von Forwarding-Tunneln und Schleifen in diesen Ketten zu behandeln

sind, ist im OMIT-Konzept mit berücksichtigt. Wird das beschriebene Verfahren eingesetzt, hat ein Subnetzwechsel eines mobilen Systems nicht mehr die Notwendigkeit einer Migration zur Folge. Diese Entkopplung des Zeitpunktes des Subnetzwechsel von dem Zeitpunkt der Migration erlaubt es, eine Migration – falls erwünscht – zu einem frei wählbaren Zeitpunkt vorzunehmen.

Ziel der nebenläufigen Migration ist es, die durch eine Migration bedingten Unterbrechungszeiten zu reduzieren. Dies wird erreicht, indem die Kommunikation in der Transportschicht auch während der Migration der Pufferinhalte zugelassen wird. Spezielle Mechanismen sind notwendig und werden vorgeschlagen, um sicherzustellen, daß die Migration ein identisches Abbild der Statusinformation, d.h. der Pufferinhalte, liefert, obwohl sich die Statusinformation bedingt durch die weiterhin aktive Transportkommunikation auch während der Migration verändert.

OMIT stellt ein Rahmenwerk dar, daß es ermöglicht den indirekten Transportansatz auch für mobile Systeme einzusetzen und trotzdem die durch die Migration bedingten Unterbrechungen nicht in Kauf nehmen zu müssen. Um diese Aufgabe zu erfüllen, müssen in einem OMIT-Transportgateway Mobile IP, das Fast-Forwarding, der Migrationsagent, in dem unter anderem das Verfahren der nebenläufigen Migration realisiert ist, und die Copy Loop, die für den Nutzdatenaustausch zwischen den beiden Transportinstanzen einer indirekten Verbindung innerhalb eines Transportgateways verantwortlich ist, miteinander interagieren. Wie diese Interaktion innerhalb eines OMIT-Transportgateways abläuft ist im vorliegenden Kapitel ebenfalls behandelt.

Kapitel 5

Implementierung und Leistungsbewertung

Gegenstand des Kapitels ist die Untersuchung und Bewertung des OMIT-Konzeptes, d.h. der Verfahren für schnelle Subnetzwechsel, des Fast-Forwarding-Konzeptes und des Konzeptes der nebenläufigen Migration. Die Untersuchungen erfolgen teils an einer prototypischen Implementierung und teils mittels Simulationen.

Da kurze Unterbrechungen nach Subnetzwechseln eine notwendige Voraussetzung sind, um überhaupt die in dieser Arbeit entwickelten Verfahren für die Migration sinnvoll einsetzen zu können, wird in Kapitel 5.1 zunächst untersucht, inwieweit sich kurze Unterbrechungen erzielen lassen. Es werden sowohl die für die Realisierung schneller Subnetzwechsel am Protokollstack des Foreign Agents bzw. des mobilen Systems vorgenommenen Änderungen als auch das den Messungen zu Grunde liegende Szenario und die Meßergebnisse beschrieben. Die für die Bewertung der nebenläufigen Migration prototypisch implementierten Komponenten und die Vermessung dieser Implementierung wird in Kapitel 5.2 beschrieben. Zusätzlich durchgeführte simulative Untersuchungen sind Gegenstand der Betrachtungen in Kapitel 5.3. In Kapitel 5.4 werden die Ergebnisse zusammengefaßt.

5.1 Evaluation der Konzepte für schnelle Subnetzwechsel

Die durch Subnetzwechsel bedingten Unterbrechungen lassen sich reduzieren, indem einerseits für eine schnelle Erkennung der Notwendigkeit eines Subnetzwechsels gesorgt wird, andererseits aber auch Optimierungen an Mobile IP vorgenommen werden. Sowohl das sogenannte *Schnelle Agent Discovery* für eine schnelle Erkennung von Subnetzwechseln als auch die für Mobile IP vorgeschlagene Fast-Forwarding-Erweiterung wurden prototypisch implementiert. Für die Messungen wurde das im folgenden Kapitel beschriebene Testbed eingesetzt.

5.1.1 Testbed

Abb. 5.1 zeigt die Konfiguration, die den Untersuchungen der Verfahren zu Grunde liegt, die für die Realisierung kurzer Unterbrechungszeiten nach Subnetzwechseln entwickelt wurden.

Der Home Agent ist an ein 100 Mbit/sec Fast Ethernet angeschlossen, bei den beiden fremden Subnetzen handelt es sich um 10 Mbit/sec Ethernet Netze. Die Foreign Agents sind direkt auf den Routern, die die Subnetze miteinander verbinden, realisiert. Die Funkanbindung des mobilen Systems ist mittels eines drahtlosen WaveLAN Netzes [Wav97] mit 2 Mbit/sec realisiert. Bei dem verwendeten WaveLAN handelt es sich nicht um das zu IEEE 802.11 konforme WaveLAN 802.11, sondern um die von Lucent Technologies vertriebene Vorgängerversion, die proprietäre Mechanismen für den Medienzugriff und die Kollisionsauflösung einsetzt und darüber hinaus auch keine Übertragungswiederholungen auf der Schicht 2 realisiert. Automatische Basisstationswechsel werden von WaveLAN im Prinzip unterstützt, allerdings umfaßten die Linux Treiber diese Funktionalität nicht. Die für automatische Basisstationswechsel notwendigen Modifikationen am Treiber wurden im Rahmen dieser Arbeit vorgenommen. Diese Modifikationen und Details zum sogenannten Beaconing der WaveLAN Basisstationen sind in Kapitel 5.1.2.1 beschrieben.

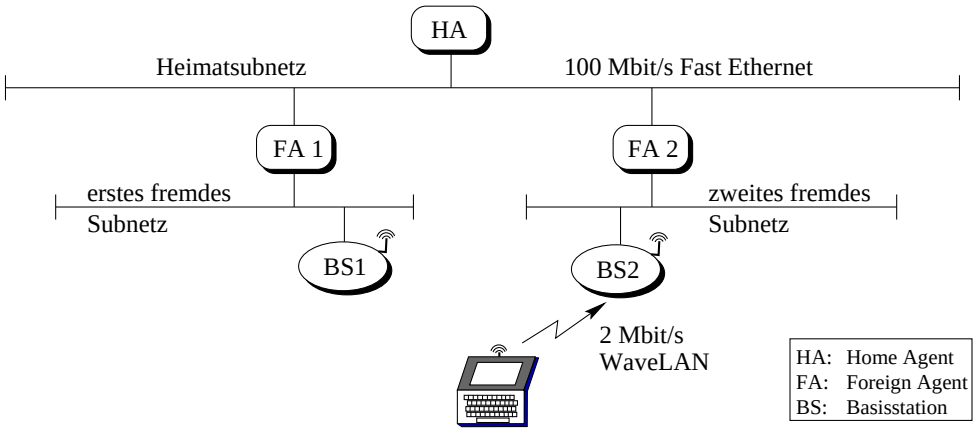


Abbildung 5.1: Testumgebung

Die Messungen unterscheiden sich teilweise dahingehend, in welchem Abstand die Basisstationen voneinander plaziert sind und hinsichtlich des Bewegungspfades des mobilen Systems. Deshalb wird bei der Beschreibung der Meßergebnisse in den jeweiligen Kapiteln noch genauer auf die Positionierung der Basisstationen eingegangen.

Für Untersuchungen von Weitverkehrsszenarien können Pakete in den Routern, die das Heimatsubnetz mit den fremden Subnetzen verbinden, künstlich verzögert werden. Diese Technik wird bei der Beschreibung der Messungen, die den Nutzen des Fast Forwardings verdeutlichen, detaillierter beschrieben.

5.1.2 Schnelles Agent Discovery

Um die Unterbrechungszeiten nach Subnetzwechseln eines mobilen Systems zu reduzieren, ist es nicht ausreichend, sich darauf zu beschränken, mittels des in Kapitel 4.5.2 beschriebenen Fast Forwardings für die schnelle Etablierung der neuen Route zu sorgen. Um die hierfür erforderlichen Mechanismen überhaupt in Mobile IP anstoßen zu können, muß zuvor der Subnetzwechsel erkannt werden.

In der Schicht 2 des mobilen Systems kann ein Basisstationswechsel erkannt werden. Da ein Basisstationswechsel zugleich auch ein notwendiges Kriterium für einen Subnetzwechsel

ist, ist es sinnvoll, einen Basisstationswechsel im mobilen System an Mobile IP zu signalisieren. Mittels Agent Solicitation Nachrichten von Mobile IP (siehe Kapitel 2.2.3.1) kann das mobile System dann ermitteln, ob nach dem Basisstationswechsel der gleiche Foreign Agent oder ein anderer Foreign Agent die Mobilitätsunterstützung des mobilen Systems übernimmt und somit auch feststellen, ob das mobile System das Subnetz gewechselt hat. Erkennt das mobile System auf diese Art einen Subnetzwechsel, so veranlaßt es mittels Mobile IP den Aufbau eines Fast-Forwarding-Tunnels zwischen dem alten und dem aktuellen Subnetz, durch den für das mobile System bestimmte Pakete an den aktuellen Aufenthaltsort geroutet werden.

Welche Informationen aus der Schicht 2 an Mobile IP signalisiert werden, hängt im Detail davon ab, wie Basisstationswechsel in dem drahtlosen Netz realisiert sind. Die folgenden Ausführungen beschreiben die Umsetzung in der prototypischen Implementierung, bei der die Anbindung eines mobilen Systems mittels des drahtlosen lokalen Netzes WaveLAN [Wav97] erfolgt.

5.1.2.1 Beacon-Auswertung in WaveLAN

Alle Basisstationen eines WaveLAN Infrastrukturnetzwerkes, zwischen denen ein mobiles System wechseln kann, nutzen den gleichen Frequenzbereich für die Übertragung. Ein mobiles System, das von einer Basisstation zu einer anderen wechselt, muß somit nicht zu einer anderen Empfangsfrequenz wechseln. Jeder Basisstation ist eine eindeutige Netzwerk-ID zugewiesen, die in der Präambel eines jeden von einer Basisstation übertragenen Pakets kodiert wird. In von einem mobilen System gesendeten Paketen ist ebenfalls die Netzwerk-ID kodiert. Diese Pakete werden von der Basisstation, die die gleiche Netzwerk-ID verwendet, nach Empfang weiterverarbeitet. Andere Basisstationen, die eine andere Netzwerk-ID nutzen, verwerfen hingegen dieses Paket. Mittels der Netzwerk-ID wird für jede Basisstation ein eigener logischer Kanal eingerichtet.

In den WaveLAN-Karten eines mobilen Systems sind zwei verschiedene Operationsmodi implementiert. Im sogenannten *Single-Modus* akzeptiert das mobile System nur Pakete mit einer bestimmten Netzwerk-ID, d.h. von einer einzigen Basisstation, im sogenannten *Multi-Modus* alle Pakete unabhängig davon, von welcher Basisstation sie gesendet wurden.

Sogenannte Beacon Pakete, in denen ebenfalls die Netzwerk-ID kodiert ist, werden alle 100 ms von den Basisstationen ausgesendet. Anhand dieser Beacons kann das mobile System die Signalqualität zu der Basisstation, von der es diese Beacons empfangen hat, beurteilen. Unterschreitet die Signalqualität einen Grenzwert, so muß das mobile System versuchen, eine besser geeignete Basisstation für die Kommunikation zu ermitteln. Da im Single-Modus Beacons anderer Basisstationen nicht empfangen werden, ist dieser hierfür nicht geeignet. Stattdessen wechselt das mobile System in den Multi-Modus und kann somit auch Beacons anderer Basisstationen empfangen und durch Auswertung der Beacons bestimmen, welche Basisstation bessere Übertragungsbedingungen bietet. Hat das mobile System eine solche Basisstation ermittelt, so meldet es sich bei dieser Basisstation an und verwendet die Netzwerk-ID dieser Basisstation in den zu sendenden Paketen, d.h. es wechselt wieder in den Single-Modus. Generell den Multi-Modus zu verwenden ist nicht praktikabel, da Paketduplikate empfangen werden und der Empfang von Paketen, die von einer Basisstation gesendet wurden, bei der das mobile System nicht angemeldet ist, unnötig Energie verbraucht.

Realisierung automatischer Basisstationswechsel in Linux
In dem verwendeten Linux Treiber für WaveLAN des PCMCIA Pakets der Version 3.0.6 kann zwar manuell die vom mobilen System zu verwendende Netzwerk-ID – und somit die Basisstation – festgelegt werden, ein automatischer Wechsel in Abhängigkeit von der Übertragungsqualität ist hingegen nicht möglich. Im Rahmen dieser Arbeit wurde die Unterstützung automatischer Basisstationswechsel zusammen mit der Beacon-Auswertung in diesen Treiber integriert.

Das Beaconing ist der Gruppe der WaveLAN Higher Protocols [Wav97] zuzuordnen. Diese Protokolle nutzen für die Übertragung der Protokolldateneinheiten die IEEE 802.2 Logical Link Control [Hal96] zusammen mit dem Subnetwork Access Protocol (SNAP) [Hal96]. Beide sind bereits im Linux Kern verfügbar und mußten somit nicht erst implementiert werden.

Um automatische Basisstationswechsel in Abhängigkeit der gemessenen Signalqualitäten der empfangenen Beacons zu ermöglichen, sind die folgenden Änderungen an dem WaveLAN Treiber [PCM98] vorgenommen worden:

- Registrierung eines SNAP Clients
  Die Funktion, die die Beacons verarbeitet, wird als SNAP Client registriert. Empfangene Beacons werden vom Linux Kern an diese Funktion zur Bearbeitung übergeben.

- Auswertung der Signalqualität der empfangenen Beacons
  Der Treiber ermittelt für die empfangenen Beacons die Signalqualität und bestimmt aus diesen Werten einen gleitenden Durchschnitt. Dieser ergibt sich als das arithmetische Mittel aus den letzten gemessenen Werten. In Abhängigkeit von diesem Durchschnitt wird entschieden, ob ein Wechsel der Basisstation vorzunehmen ist.

- Zusätzliche IOCTLs
  Um im mobilen System Mobile IP über Basisstationswechsel informieren zu können, sind zusätzliche IOCTLs notwendig. Die IOCTLs sind für die Kommunikation zwischen dem im Betriebssystemkern realisierten WaveLAN Treiber und dem im User Space implementierten Mobile IP erforderlich. Eine detailliertere Beschreibung der Interaktion des Treibers mit Mobile IP erfolgt in Kapitel 5.1.2.2. Ein weiterer IOCTL ermöglicht es, die Auswertung der Beacons und automatische Basisstationswechsel eines mobilen Systems zu aktivieren bzw. zu deaktivieren.

Zusammen mit jedem empfangenen Paket stellt die WaveLAN-Hardware Werte zur Verfügung, die das Signal-Rausch-Verhältnis im Wertebereich [0-15] und die Signalstärke im Wertebereich [0-34] wiedergeben.

Bestimmung eines Wechselkriteriums
Für die Entscheidung, ob ein Basisstationswechsel vorzunehmen ist, ist ein geeignetes Kriterium erforderlich. Zunächst wird betrachtet, ob sich das Signal-Rausch-Verhältnis oder die Signalstärke besser als Wechselkriterium eignet. In einem weiteren Schritt werden geeignete Grenzwerte ermittelt. Den im folgenden beschriebenen Messungen liegt die in Kapitel 5.1.1 beschriebene Netztopologie zu Grunde. Die Basisstationen sind in einem Bürogebäude mit Stahlbetonwänden ca. 29 Meter voneinander entfernt angeordnet. Darüber hinaus befindet sich Basisstation 1 im Erdgeschoß, während Basisstation 2 im Keller angeordnet ist.

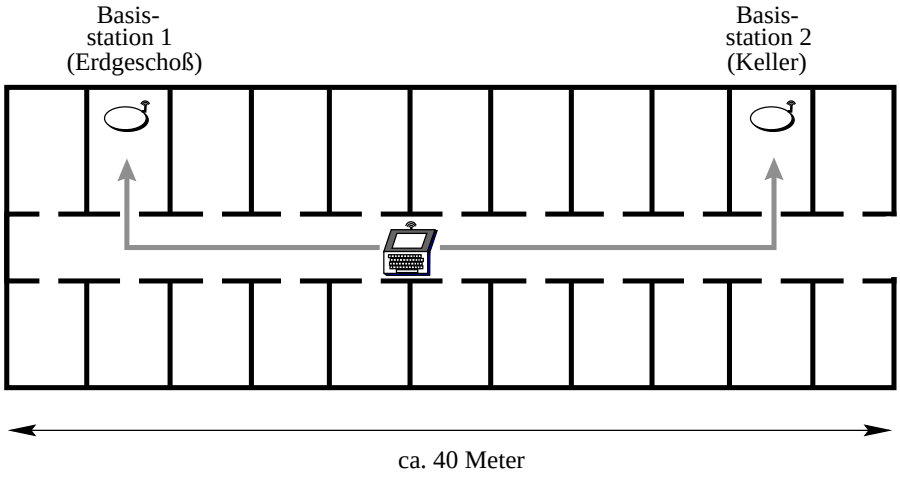


Abbildung 5.2: Bewegungspfad des mobilen Systems

Abb. 5.2 zeigt die örtlichen Gegebenheiten und den Pfad, auf dem das mobile System zwischen Basisstation 1 und Basisstation 2 bewegt wird. Die maximale Annäherung an Basisstation 1 beträgt 2 Meter, die an die zweite Basisstation 5 Meter.

Um während der gesamten Messung die Signalstärke nicht nur jeweils einer sondern beider Basisstationen auswerten zu können, wurde der WaveLAN-Treiber dahingehend geändert, daß auch im Single-Modus die Signalstärke der Basisstationen, bei denen das mobile System nicht angemeldet ist, ausgewertet werden können. Diese Strategie ist in der Praxis nicht einsetzbar, ermöglicht aber einen Vergleich der Signalstärken der Beacons beider Basisstationen.

Abb. 5.3 zeigt wie sich die Signalstärke bzw. das Signal-Rausch-Verhältnis der empfangenen Beacons verändert, wenn sich das mobile System von Basisstation 1 kommend bis auf 5 Meter an Basisstation 2 annähert ($t = 45\ sec$) und dann wieder zurück zu Basisstation 1 bewegt. Ein Glättung der Kurven wird erreicht, indem für das Signal-Rausch-Verhältnis der gleitende Mittelwert aus den letzten 5 Meßwerten und für die Signalstärke der Mittelwert aus den letzten 7 Meßwerten aufgetragen wird. Anhand von in den Beacons kodierten Sequenznummern kann der Verlust von Beacons erkannt werden. Nicht empfangene Beacons gehen mit dem Wert 0 für das Signal-Rausch-Verhältnis in die Mittelwertbildung ein.

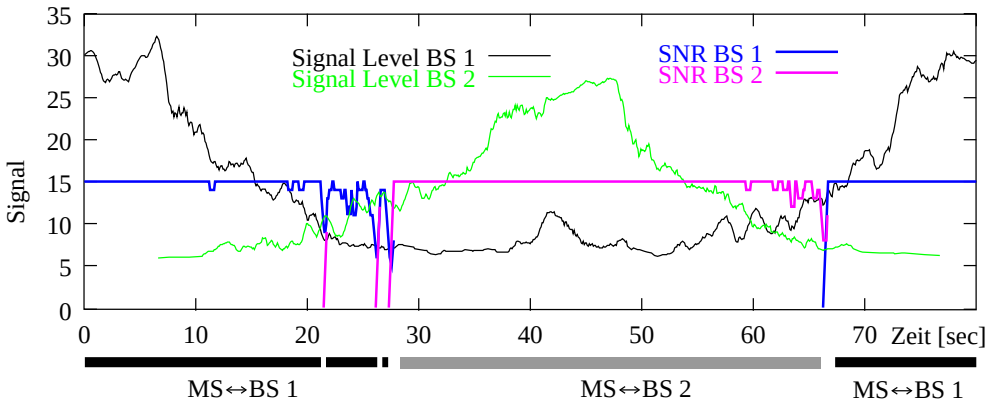


Abbildung 5.3: Signal-Rausch-Verhältnis und Signalstärke empfangener Beacons

Die Betrachtung der Signalstärken, die anhand der von Basisstation 1 bzw. Basisstation 2

ausgesendeten Beacons bestimmt werden, zeigt, daß es sinnvoll ist, im Zeitintervall $[20, 30]$ den Wechsel zu Basisstation 2 vorzunehmen. Der Vergleich der Signalstärke der Beacons von Basisstation 1 und Basisstation 2 ist aber normalerweise, d.h. ohne die in der Praxis nicht einsetzbaren, für diese Messungen am WaveLAN Treiber vorgenommenen Änderungen nicht möglich, da wegen des Single-Modus nur Beacons der Basisstation 1 empfangen werden können. Es stellt sich somit die Frage, wie alleine durch Auswertung der von Basisstation 1 empfangenen Beacons der Zeitpunkt für einen Basisstationswechsel bestimmt werden kann.

Da der gleitende Durchschnitt der Signalstärken der von Basisstation 1 empfangenen Beacons im Zeitraum $[20, 30]$ nicht signifikant einbricht, ist er nicht als Kriterium für die Notwendigkeit eines Basisstationswechsels einsetzbar. Der gleitende Durchschnitt des Signal-Rausch-Verhältnisses hingegen bleibt bis zum Zeitpunkt $t = 22$ nahezu konstant auf dem Maximalwert 15 und bricht dann deutlich ein. Das Signal-Rausch-Verhältnis kann somit als Kriterium für die Notwendigkeit eines Basisstationswechsels verwendet werden.

Um automatische Basisstationswechsel zu realisieren, muß ein geeigneter Grenzwert für den gleitenden Mittelwert des Signal-Rausch-Verhältnisses festgelegt werden, bei dessen Unterschreiten dann ein Basisstationswechsel veranlaßt wird. Da weiterhin Oszillationen zwischen zwei Basisstationen – wegen des Schwankens des Signal-Rausch-Verhältnis um den Grenzwert – zu vermeiden sind, werden zwei Grenzwerte verwendet: Ein unterer Grenzwert, bei dessen Unterschreiten das mobile System in den Multi-Modus wechselt und mit der Suche nach einer neuen Basisstation beginnt, und ein oberer Grenzwert, bei dessen Überschreiten das mobile System sich bei einer Basisstation anmeldet und wieder in den Single-Modus zurückwechselt. Bei der Vermessung verschiedener Szenarien haben sich die Werte 10 bzw. 12 als geeignete Werte für den unteren bzw. oberen Grenzwert herauskristallisiert. Wie unter Berücksichtigung dieser beiden Grenzwerte der Wechsel des mobilen Systems von Basisstation 1 zu Basisstation 2 im Zeitraum $[20, 30]$ erfolgt, wird im folgenden diskutiert.

Das Signal-Rausch-Verhältnis ist nur für solche Beacons in Abb. 5.3 aufgetragen, die das mobile System im Single-Modus bzw. Multi-Modus empfangen kann. Zusätzlich kann der Abbildung anhand der unterhalb des Schaubildes eingezeichneten Teilstrecken entnommen werden, in welchen Zeiträumen das mobile System bei welcher Basisstation angemeldet war. Während der schwarz dargestellten Zeiträume war es bei Basisstation 1 angemeldet, während grau eingezeichneter Zeiträume bei Basisstation 2. Weiße Bereiche reflektieren Zeitphasen, während der das mobile System im Multi-Modus war, d.h. Pakete von beiden Basisstationen empfangen hat.

Abb. 5.4 zeigt im Detail wie sich das als Kriterium für einen Basisstationswechsel herangezogene Signal-Rausch-Verhältnis im relevanten Zeitraum $[21, 28]$ entwickelt. In Abb. 5.4a ist ein dreimaliger Wechsel des mobilen Systems in den Multi-Modus zu erkennen, bevor es sich zum Zeitpunkt $t = 27.7$ endgültig bei der Basisstation 2 anmeldet.

In Abb. 5.4b ist das Signal-Rausch-Verhältnis der von Basisstation 1 bzw. Basisstation 2 empfangenen Beacons im Zeitraum $[20.5, 22.5]$ dargestellt. Zum Zeitpunkt $t = 21.55$ unterschreitet das Signal-Rausch-Verhältnis der von Basisstation 1 empfangenen Beacons den Grenzwert 10. Das mobile System wechselt daraufhin in dem Multi-Modus und empfängt bis zum Zeitpunkt $t = 21.7$ drei Beacons mit dem Signal-Rausch-Verhältnis 15 von der Basisstation 2. Da für nicht empfangene Beacons bei der Berechnung des gleitenden Mittelwerts der Wert 0 eingesetzt wird, ergibt sich ein gleitender Mittelwert von 3, 6 bzw. 9. Bevor das mobile System das nächste Beacon von Basisstation 2 empfängt, überschreitet zum Zeitpunkt

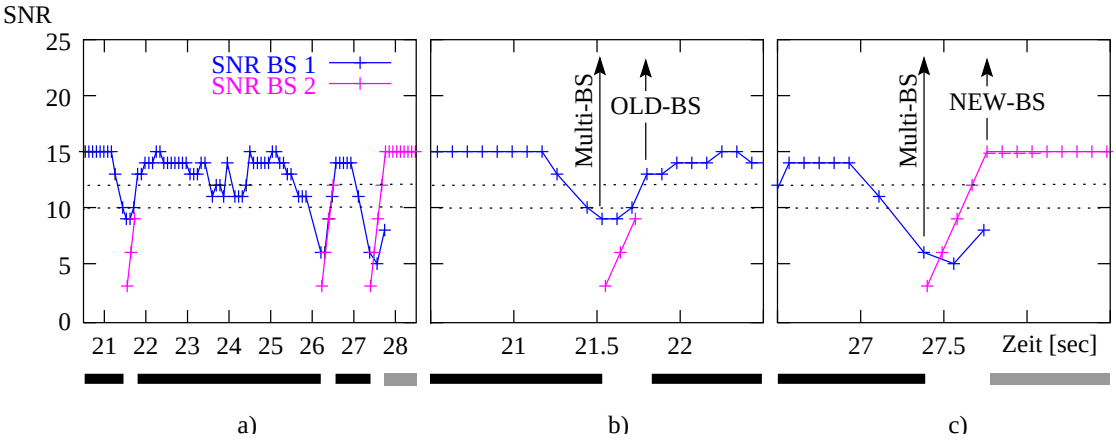


Abbildung 5.4: Detailausschnitte: Signal-Rausch-Verhältnis

$t = 27.75$ der gleitende Mittelwert von Basisstation 1 den Grenzwert 12. Das mobile System wechselt somit wieder in den Single-Modus zurück zu Basisstation 1 und empfängt keine weiteren Beacons von Basisstation 2. Es wird im betrachteten Zeitraum somit kein Wechsel zu Basisstation 2 vollzogen. Analog ist die Situation im Zeitraum $[26, 26.5]$. Auch in diesem Zeitraum wechselt das mobile System in den Multi-Modus, kehrt aber danach ebenfalls in den Single-Modus und zu Basisstation 1 zurück.

Abb. 5.4c zeigt die Situation, in der das mobile System erst in den Multi-Modus und anschließend in den Single-Modus zu der Basisstation 2 wechselt. Da zum Zeitpunkt $t = 27.7$ der gleitende Mittelwert des Signal-Rausch-Verhältnisses der von der Basisstation 2 empfangen Beacons den Grenzwert 12 überschreitet, wechselt das mobile System in den Single-Modus zu Basisstation 2 und empfängt keine weiteren Beacons von der Basisstation 1.

In Abb. 5.4b und Abb. 5.4c sind zusätzlich die Signale dargestellt, die an Mobile IP gesendet werden. Auf sie wird im folgenden Abschnitt eingegangen.

5.1.2.2 Signalisierung aus dem WaveLAN-Treiber an Mobile IP

Mittels der beschriebenen Mechanismen kann der modifizierte WaveLAN-Treiber des mobilen Systems bestimmen, wann ein Basisstationswechsel vorliegt. Der Treiber sendet daraufhin an den Mobile IP Prozeß ein Unix-Signal, das Mobile IP darüber informiert, daß vom Treiber die Netzwerk-ID geändert wurde. Das Signal selbst informiert nicht darüber, aus welchem Grund das Signal gesendet wurde. Über einen IOCTL, der im WaveLAN-Treiber zusätzlich implementiert ist, kann Mobile IP die Ursache für das Signal ermitteln. Folgende Ursachen sind möglich:

- MULTI-BS
  Das mobile System ist in den Multi-Modus gewechselt, um Signalstärken verschiedener Basisstationen auswerten und die Entscheidung treffen zu können, ob ein Basisstationswechsel vorzunehmen ist.

- OLD-BS
  Das WaveLAN System ist, nachdem es in den Multi-Modus gewechselt ist, zurück zu der

Basisstation gewechselt, bei der es vor dem Wechsel in dem Multi-Modus angemeldet war.

- NEW-BS
  Das mobile System ist, nachdem WaveLAN in den Multi-Modus gewechselt ist, zu einer anderen Basisstation gewechselt.

5.1.2.3 Verarbeitung der Signale in Mobile IP

Abb. 5.5 zeigt das Zustandsübergangsdiagramm, das die Verarbeitung der Signale in Mobile IP beschreibt. Da die hierfür notwendigen Änderungen an Mobile IP nicht im direkten Zusammenhang mit den bereits in Kapitel 4.5.2 beschriebenen Fast-Forwarding-Erweiterungen von Mobile IP stehen, sind sie nicht dort beschrieben, sondern werden erst im folgenden genauer betrachtet.

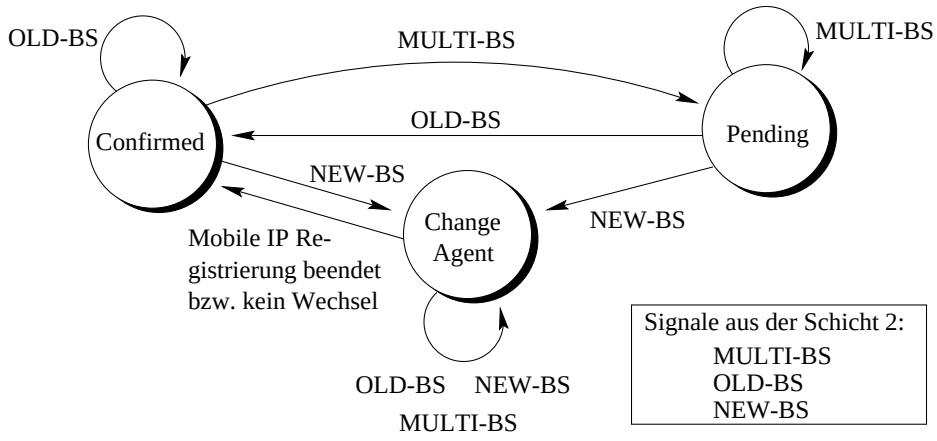


Abbildung 5.5: Verarbeitung der Signale in Mobile IP

Im Zustand „Confirmed“ befindet sich Mobile IP, falls das mobile System bei einem Foreign Agent des Subnetzes registriert ist und darüber hinaus WaveLAN im Single-Modus operiert. Der Zustand „Pending“ reflektiert, daß WaveLAN im Multi-Modus betrieben wird. Seitens Mobile IP werden in diesem Zustand noch keine nach einem Subnetzwechsel notwendigen Aktionen veranlaßt. Im Zustand „Change Agent“ operiert WaveLAN im Single-Modus, und Mobile IP ist über den Subnetzwechsel informiert. Mobile IP veranlaßt daraufhin in diesem Zustand die nach einem Subnetzwechsel erforderlichen Aktionen. Der Subnetzwechsel ist aber noch nicht abgeschlossen.

Der Übergang zwischen den drei möglichen Zuständen erfolgt in Abhängigkeit davon, welche der drei oben genannten möglichen Ursachen für das an Mobile IP gesandte Signal verantwortlich ist.

Wechselt WaveLAN auf dem mobilen System auf Grund einer Unterschreitung des unteren Grenzwertes des Signal-Rausch-Verhältnisses in den Multi-Modus, erfolgt ein Übergang aus dem Zustand „Confirmed“ in den Zustand „Pending“. Im Zustand „Pending“ empfängt Mobile IP auf Grund des Multi-Modus von WaveLAN eventuell Agent Advertisements von Foreign Agents aus verschiedenen Subnetzen. Da zu diesem Zeitpunkt nicht klar ist, ob WaveLAN zu einer neuen Basisstation wechselt oder wieder im Single-Modus bei der alten Basisstation betrieben wird, macht es keinen Sinn, bereits zu diesem Zeitpunkt einen Subnetzwechsel

einzuleiten. Aus diesem Grunde ignoriert Mobile IP empfangene Agent Advertisements im Zustand „Pending“. Der Zustand „Pending“ wird verlassen, falls sich das mobile System wieder bei der alten Basisstation registriert (Ereignis OLD-BS). Es erfolgt ein Übergang in den Zustand „Confirmed“. Im Falle eines Wechsels zu einer neuen Basisstation (Ereignis NEW-BS) wird von Mobile IP mittels einer Agent-Solicitation-Nachricht geprüft, ob ein Subnetzwechsel vorliegt, und in den Zustand „Change Agent“ gewechselt. Liegt kein Subnetzwechsel vor, erfolgt ein Übergang in den Zustand „Confirmed“, andernfalls wird die Registrierung des mobilen Systems im neuen Subnetz veranlaßt und erst nach Abschluß der Registrierung in den Zustand „Confirmed“ gewechselt. Signalisiert WaveLAN im Zustand „Change Agent“, in dem Mobile IP eine Registrierung veranlaßt, aber noch nicht abgeschlossen hat, einen erneuten Basisstationswechsel, so bleibt Mobile IP im Zustand „Change Agent“ und nimmt eine erneute Registrierung vor.

Es werden nicht nur automatische sondern auch manuelle Basisstationswechsel unterstützt. Mittels manueller Wechsel lassen sich skriptgesteuert zu reproduzierbaren Zeitpunkten Basisstationswechsel vornehmen. Im Falle eines manuellen Basisstationswechsels erfolgt der Basisstationswechsel, ohne daß WaveLAN in einer Zwischenphase im Multi-Modus betrieben wird. Die Übergänge aus dem Zustand „Confirmed“ nach Empfang eines OLD-BS bzw. NEW-BS Signals reflektieren dies.

5.1.2.4 Zeitdauer bis zum Erkennen eines Subnetzwechsels

Wieviel Zeit zwischen einem Basisstationswechsel und dem Start der vom mobilen System veranlaßten Registrierung beim Home Agent vergeht, ist in Tabelle 5.1 aufgeführt. Bei den in der Tabelle aufgeführten Werten wird davon ausgegangen, daß die erforderlichen Agent Solicitation bzw. Agent Advertisement Nachrichten beim ersten Sendeversuch erfolgreich übertragen werden.

Verzögerung	Ohne Schicht 2 Unterstützung	Mit Schicht 2 Unterstützung
Minimal	0 ms	5 ms
Maximal	1000 ms	50 ms
Durchschnitt	500 ms	ca. 25 ms

Tabelle 5.1: Verzögerung bis zum Erkennen eines Subnetzwechsels

Bei der Variante ohne Schicht 2 Unterstützung kann das mobile System lediglich anhand der periodisch alle 1000 ms vom Mobility Agent ausgesendeten Agent Advertisements einen Subnetzwechsel erkennen. Bestenfalls empfängt es unmittelbar nach einem Basisstationswechsel das Advertisement und kann dann sofort den Subnetzwechsel erkennen. Schlimmstenfalls vergehen 1000 ms bis zum nächsten empfangenen Advertisement und deshalb auch 1000 ms, bis der Subnetzwechsel festgestellt wird.

In der Variante mit Schicht 2 Unterstützung wird sofort nach dem Basisstationswechsel ermittelt, ob ein Subnetzwechsel stattgefunden hat. Sobald das vom Foreign Agent nach Empfang der Agent Solicitation gesendete Agent Advertisement vom mobilen System empfangen wird, hat dieses Kenntnis, ob ein Subnetzwechsel stattgefunden hat. Die für diese beiden

Pakete erforderliche Übertragungsdauer bestimmt die Zeitdauer bis zum Erkennen eines Subnetzwechsels. Die Vermessung der prototypischen Implementierung [Die98] ergab – abhängig vom Hintergrundverkehr – Zeitdauern zwischen 5 ms und 50 ms.

Wird das Agent Advertisement beim ersten Übertragungsversuch nicht erfolgreich zum mobilen System übertragen, so vergehen bei der Variante ohne Schicht 2 Unterstützung weitere 1000 ms bis das nächste Advertisement übertragen wird und dann ggf. der Subnetzwechsel erkannt werden kann. Bei der Variante mit Schicht 2 Unterstützung, d.h. mit Signalisierung an Mobile IP, kann das mobile System den vermeintlichen Verlust eines Agent Advertisements erkennen und unter der Kontrolle eines Timers sofort mittels eines Agent Solicitations erneut anfordern. Es ist somit robuster gegen Paketverluste. Subnetzwechsel können deutlich schneller als bei der Variante ohne Schicht 2 Unterstützung festgestellt werden.

5.1.3 Fast Forwarding

Die im letzten Kapitel beschriebenen Messungen belegen, daß mittels des Schnellen Agent Discoverys zusammen mit der Signalisierung aus der Schicht 2 unmittelbar nach einem Basisstationswechsel ein Subnetzwechsel erkannt und daraufhin die Registrierung beim Home Agent veranlaßt werden kann. Inwieweit auch das Fast Forwarding zu einer Reduktion der Unterbrechungszeiten beitragen kann, ist Gegenstand der im folgenden beschriebenen Untersuchungen.

5.1.3.1 Modifikationen an der Mobile IP Implementierung

Die Implementierung des Fast-Forwarding-Konzeptes erfolgte im Rahmen einer Diplomarbeit [Die98], die sich über das Fast-Forwarding-Konzept hinausgehend mit Aspekten der Ressourcenreservierung für mobile Systeme beschäftigte. Das Fast-Forwarding-Konzept wurde in die an der State University of New York, Binghamton, entstandene Mobile IP Implementierung [GD96] für das Betriebssystem Linux integriert.

Änderungen am mobilen System
Das mobile System übergibt in der Registrierungsanforderung zusätzlich die IP-Adresse des alten Foreign Agents an den neuen Foreign Agent. Hierzu wird die im Anhang in Abschnitt A.1 beschriebene alte-Foreign-Agent-Erweiterung an eine Registrierungsanforderung an Mobile IP angehängt.

Änderungen am Foreign Agent
Die Implementierung des Foreign Agents wurde dahingehend geändert, daß sie das in Kapitel 4.5.2.1 mittels eines Zustandsübergangsdiagramms beschriebene Verhalten reflektiert. Darüber hinaus wurde die Protokollverarbeitung für die in Anhang A.1 beschriebenen Nachrichten des Fast-Forwarding-Protokolls, das zwischen Foreign Agents operiert, integriert.

5.1.3.2 Einfluß des Fast Forwardings auf UDP-Ströme

Den in diesem Abschnitt beschriebenen Messungen liegt ebenfalls das in Kapitel 5.1.1 vorgestellte Szenario zugrunde. Um auch Weitverkehrsszenarien nachbilden zu können – insbeson-

dere längere Paketlaufzeiten zwischen dem Home Agent und dem mobilen System – wurden die beiden Router, die die fremden Subnetze mit dem Heimatsubnetz verbinden, mit einer Paketverzögerung für zu routende IP-Pakete versehen.

Dies wurde im Kernel realisiert und ermöglicht eine optionale Verzögerung von IP-Paketen um eine einstellbare Zeitdauer. Es werden lediglich IP-Pakete verzögert, deren Quelle oder deren Ziel das Heimatsubnetz ist. Pakete, die von einem fremden Subnetz in das andere fremde Subnetz übertragen werden, erfahren keine Verzögerung. Es wird somit ein Szenario nachgebildet, bei dem zwei fremde Subnetze geographisch einander nahe liegen, aber beide Subnetze weit vom Heimatsubnetz des betrachteten mobilen Systems entfernt sind. Zwischen Heimatsubnetz und fremdem Subnetz übertragene Pakete werden jeweils um 100 ms verzögert. Somit ergibt sich für zwischen dem mobilen System und dem Heimatsubnetz übertragene Pakete eine minimale Paketumlaufzeit von 200 ms.

Um den Einfluß von Übertragungsfehlern und Paketverlusten der Funkstrecke auf die Meßergebnisse zu minimieren, sind für diese Messungen die Basisstationen nicht wie in Abb. 5.2 dargestellt ca. 29 Meter voneinander entfernt plaziert, sondern zusammen mit dem mobilen System in ein und demselben Büro angeordnet. Es liegt aber weiterhin die in Abb. 5.1 skizzierte Netztopologie vor.

Auf Grund der räumlichen Nähe der beiden Basisstationen und des mobilen Systems sind keine automatischen Basisstationswechsel seitens des mobilen Systems möglich. Sie werden stattdessen manuell durch gezielte Wahl der Netzwerk-ID der jeweiligen Basisstation auf dem mobilen System nachgebildet. Diese Vorgehensweise bietet den Vorteil deterministisch reproduzierbarer Basisstationswechsel zu bestimmten Zeitpunkten.

Messungen

Eine auf dem Home Agent laufende Anwendung erzeugt einen 64 kbit/s Audio-Datenstrom. Dieser Datenstrom wird in UDP-Paketen, die jeweils 160 Bytes Audio-Daten transportieren, zum mobilen System übertragen. Vom Sender wird alle 20 ms ein Audio-Datenpaket an das Netzwerk übergeben. Im stationären Fall, d.h. falls das mobile System das Subnetz nicht wechselt, empfängt es auch alle 20 ms ein Audio-Datenpaket. Besonderes Augenmerk bei den folgenden Betrachtungen liegt auf den Zeitpunkten, zu denen das mobile System die Basisstation und im betrachteten Szenario somit auch das Subnetz wechselt. Es sind dies die Zeitpunkte 12, 24, 35, 47 und 59.

Abb. 5.6a zeigt das Szenario ohne Fast Forwarding, Abb. 5.6b dasjenige mit Fast Forwarding. Auf der x-Achse ist jeweils die Zeitdauer seit dem Start der Messung aufgetragen, auf der y-Achse die Zeit, die seit dem Empfang des letzten Audio-Datenpakets vergangen ist.

Es ist deutlich zu erkennen, daß bei der Variante ohne Fast Forwarding nach Subnetzwechseln für ca. 200 ms bis 230 ms keine Audio-Datenpakete von dem mobilen System empfangen werden können. Die Ursache liegt darin, daß der Home Agent erst dann an das mobile Systeme adressierte Pakete in das neue Subnetz tunneln kann, sobald er durch eine Mobile IP Registrierung von dem Subnetzwechsel erfahren hat. Auf Grund der Paketlaufzeit der Registrierung zwischen dem mobilen System und dem Home Agent ergibt sich eine Verzögerung von 100 ms, weitere 100 ms vergehen, bis das erste in das neue Subnetz getunnelte Paket vom mobilen System empfangen werden kann. Es ergibt sich somit beim Ansatz ohne Fast Forwarding minimal eine Unterbrechung des Datenstroms von der Dauer einer RTT, d.h. von

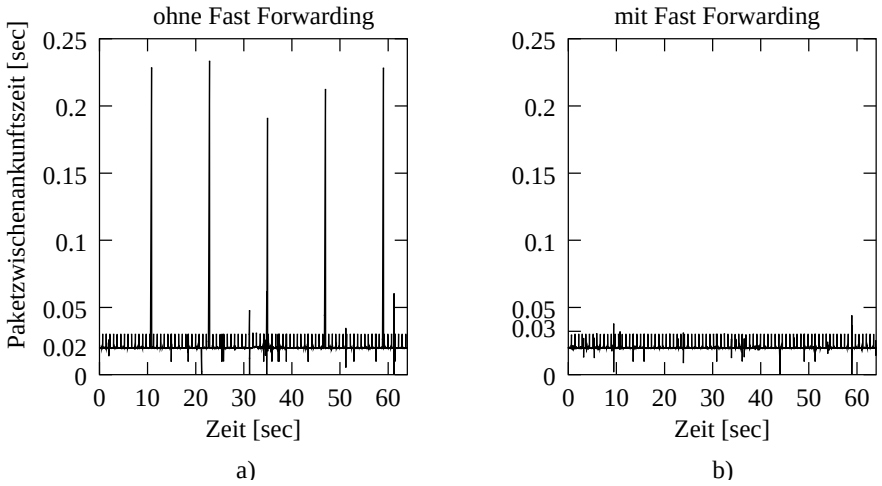


Abbildung 5.6: Auswirkungen von Unterbrechungen auf einen UDP-Datenstrom

200 ms. Die während dieser Zeitdauer noch in das alte Subnetz ausgelieferten Audio-Datenpakete werden nicht zum mobilen System ausgeliefert, sondern von diesem als Paketverluste registriert.

In Abb. 5.6b sind hingegen keine nennenswerten Unterbrechungen im Datenstrom zu beobachten. Für die Wiederherstellung der Netzwerkanbindung des mobilen Systems muß im Falle des Fast Forwardings lediglich der neue Foreign Agent den alten Foreign Agent über den Subnetzwechsel des mobilen Systems informieren und dieser daraufhin den Fast-Forwarding-Tunnel einrichten. Da die Übertragungszeit eines Pakets zwischen dem alten und dem neuen Foreign Agent im Vergleich zur Übertragungszeit zum Home Agent deutlich kürzer ist, ist die Unterbrechungsdauer des Audio-Datenstroms und die Anzahl der Paketverluste ebenfalls deutlich geringer.

Die in Abb. 5.6b erkennbaren Schwankungen der Paketzwischenankunftszeiten im Bereich zwischen 20 ms und 30 ms ergibt sich durch den künstlich – für die Nachbildung eines Weitverkehrsszenarios – eingeführten Delay auf den Routern. Dieser künstliche Delay schwankt auf Grund der minimalen Granularität von 10 ms für Timer im Betriebssystem Linux [BBD+99] um bis zu 10 ms. Dies führt zu den zwischen 20 ms und 30 ms schwankenden Paketzwischenankunftszeiten, obwohl eigentlich eine nahezu konstante Paketankunftszeit von 20 ms zu erwarten wäre. Die sich aus der Granularität von 10 ms für Timer im Betriebssystem Linux ergebenden Schwankungen sind auch bei den in [Sch00] beschriebenen Messungen erwähnt.

5.1.3.3 Einfluß des Fast Forwardings auf Ende-zu-Ende TCP-Verbindungen

Obwohl das Fast-Forwarding-Konzept in dieser Arbeit primär im Kontext einer optimierten Mobilitätsunterstützung für den indirekten Transportansatz entwickelt wurde, bietet es auch Vorteile für Ende-zu-Ende TCP-Verbindungen. Im folgenden wird betrachtet, welche Auswirkungen die wesentlichen Merkmale des Fast-Forwarding-Konzeptes auf Ende-zu-Ende TCP-Verbindungen haben. Es sind dies

- das geänderte Routing über den alten Foreign Agent und
- die kürzeren Unterbrechungen nach Subnetzwechseln.

Da davon auszugehen ist, daß der alte Foreign Agent und der neue Foreign Agent nicht weit voneinander entfernt sind, hat das Routing Home Agent → alter Foreign Agent → neuer Foreign Agent (Mobile IP mit Fast Forwarding) keine signifikant längere Paketlaufzeit als das Routing Home Agent → neuer Foreign Agent (Mobile IP ohne Fast Forwarding) zur Folge. Das geänderte Routing in Mobile IP mit Fast Forwarding hat aus diesem Grunde keine wesentlichen Auswirkungen auf eine Ende-zu-Ende TCP-Verbindung.

Die im Fall von Mobile IP mit Fast Forwarding im Vergleich zu Mobile IP ohne Fast Forwarding kürzeren Unterbrechungszeiten wirken sich positiv auf die TCP-Ende-zu-Ende Verbindungen aus. Es ergibt sich bei Einsatz des Fast Forwardings eine geringere Anzahl von Paketverlusten. Wie sich dies auf TCP auswirkt, zeigt der in Abb. 5.7 dargestellte Verlauf der Sequenznummern.

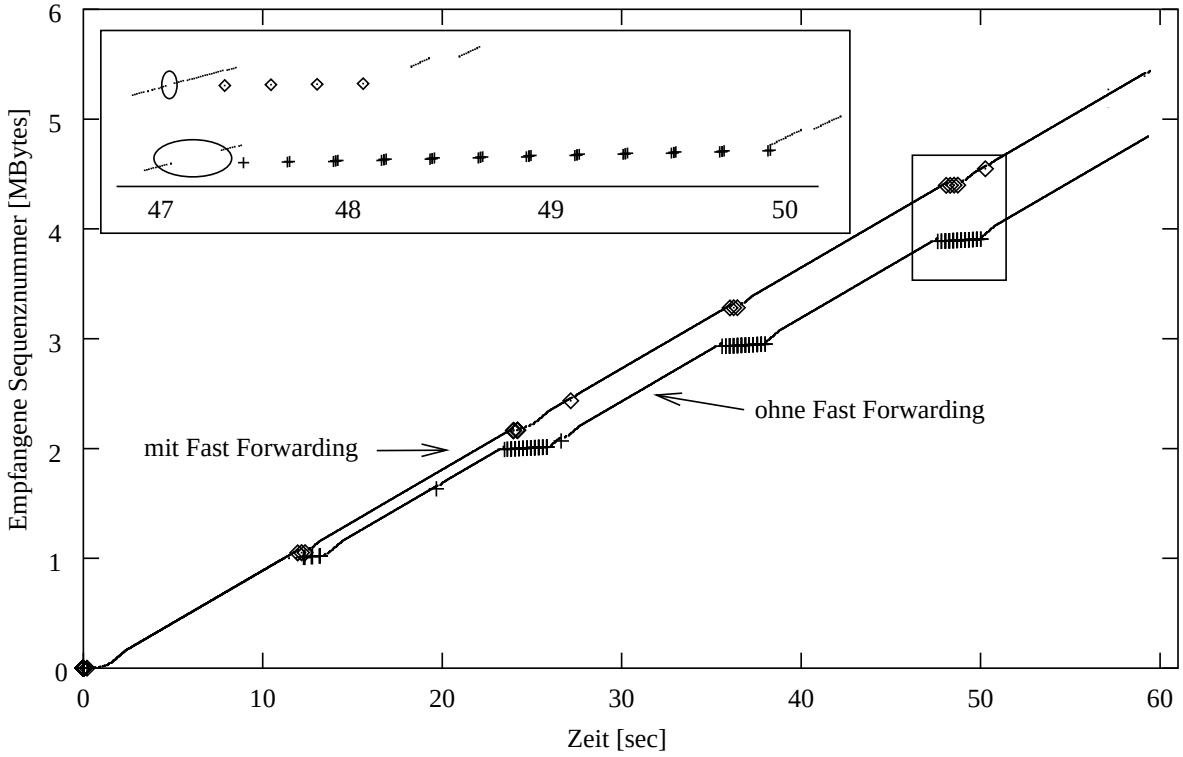


Abbildung 5.7: Auswirkungen von Unterbrechungen auf einen TCP-Datenstrom

Der Messung liegt das in Kapitel 5.1.3.2 beschriebene Szenario mit der in Abb. 5.1 dargestellten Netztopologie zu Grunde. Sowohl der Sender als auch der Empfänger verwenden selektive Bestätigungen in der TCP-Instanz. Auf dem Home Agent erzeugt eine Anwendung alle 10 ms Nutzdateneinheiten der Größe 1000 Bytes und übergibt diese an TCP zur Übertragung zum mobilen System. Ohne durch Subnetzwechsel bedingte Unterbrechungen steigt die erfolgreich übertragene Datenmenge linear mit der Zeit, da Übertragungsfehler wegen der räumlichen Nähe der Basisstationen und des mobilen Systems zu vernachlässigen sind.

Abb. 5.7 zeigt die Sequenznummernentwicklung für den Fall, daß alle 12 Sekunden ein Subnetzwechsel stattfindet. Auf der x-Achse ist die seit dem Start der TCP-Verbindung vergangene Zeit aufgetragen. Die y-Achse repräsentiert die Sequenznummern der vom mobilen System empfangenen TCP-Pakete. Die Sequenznummer eines empfangenen Pakets wird durch einen Punkt dargestellt. Übertragungswiederholungen sind durch ein Quadrat (Fast Forwarding) bzw. ein Kreuz (kein Fast Forwarding) kenntlich gemacht.

Kommt das Fast-Forwarding-Verfahren zum Einsatz, so ergibt sich im beschriebenen Szenario nach 60 Sekunden ein um ca. 10 Prozent höherer Durchsatz als beim Verzicht auf das Fast Forwarding. Um das Verhalten von TCP nach einem Subnetzwechsel studieren zu können, ist in Abb. 5.7 ein Detailausschnitt der Sequenznummernentwicklung während des Zeitraumes [47, 50] dargestellt. Deutlich zu erkennen ist, daß die durch Ellipsen kenntlich gemachte Dauer der durch Mobile IP bedingten Unterbrechung bei der Variante mit Fast Forwarding signifikant kürzer ist als bei der Variante ohne Fast Forwarding. Es gehen 4 bzw. 21 TCP-Nutzdatenpakete während der Unterbrechung verloren.

Die notwendigen Übertragungswiederholungen können ebenfalls der Ausschnittvergrößerung entnommen werden. Bei der Variante mit Fast Forwarding wird das erste Paket mittels der Fast-Recovery-Strategie von TCP wiederholt. Nach der durch den Subnetzwechsel bedingten Unterbrechung von ca. 20 ms, generiert die TCP-Instanz im Empfänger Bestätigungsduplikate, die nach 100 ms beim Sender eintreffen. Der Sender wiederholt daraufhin das entsprechende Paket und reduziert das Lastkontrollfenster um den Faktor zwei. Nach weiteren 100 ms, d.h. 200 ms nach Ende der Unterbrechung, trifft das wiederholte Paket beim Empfänger ein. Das reduzierte Lastkontrollfenster kann dazu führen, daß für die selektive Übertragungswiederholung von Paketen kein Kredit mehr verfügbar ist. In diesem Falle wird genau ein Paket pro Paketumlaufzeit wiederholt und somit die erneute Übertragung unnötig lange verzögert. Der dargestellte Sequenznummernverlauf zeigt allerdings deutlich, daß nach der ersten Übertragungswiederholung nicht wiederholte Datenpakete übertragen wurden. Obwohl der Sender eigentlich durch die selektiven Bestätigungen hätte erkennen müssen, daß weitere drei Übertragungswiederholungen notwendig sind, überträgt er andere Datenpakete. Dieses Verhalten des Linux Kernels (Version 2.1.97), neue Pakete bevorzugt vor zu wiederholenden Paketen zu übertragen, erscheint fragwürdig.

Die untere Kurve im Detailausschnitt zeigt den Sequenznummernverlauf, falls auf die Fast-Forwarding-Strategie verzichtet wird. Die Unterbrechung von ca. 200 ms bewirkt, daß das erste fehlende Datenpaket nicht mittels Fast Recovery wiederholt werden kann, sondern beim Sender ein Timeout erfolgt. Als unmittelbare Folge davon setzt der Sender das Lastkontrollfenster auf 1. Während des nachfolgenden Slow Starts wird das Fenster exponentiell geöffnet. In Abb. 5.7 enthält der erste Burst wiederholter Pakete ein Paket, der zweite zwei Pakete und alle weiteren Bursts vier Pakete. Das Lastkontrollfenster wird im beschriebenen Szenario nicht über die Größe vier hinaus geöffnet, da ein Burst jeweils nur zwei neue Datenpakete und zwei Übertragungswiederholungen enthält.

Der wesentliche Nutzen des Fast-Forwarding-Konzeptes im Kontext von Ende-zu-Ende TCP-Verbindungen ist, daß wegen der kürzeren Unterbrechungen nach Subnetzwechsel Übertragungswiederholungen mittels Fast Recovery erfolgen können und eine Reduktion des Lastkontrollfensters auf den Wert 1 vermieden werden kann. Wird auf das Fast Forwarding verzichtet, gehen während der länger andauernden Unterbrechung alle Pakete verloren. Somit kann der Empfänger keine Bestätigungsduplikate generieren und keine Paketwiederholung mittels Fast Retransmit veranlassen. Der Sender veranlaßt erst nach dem Timeout die Übertragungswiederholung und reduziert darüber hinaus das Lastkontrollfenster auf den Wert 1. Insgesamt hat bei der Mobile IP Variante ohne Fast Forwarding der Subnetzwechsel für eine Dauer von ca. 3 Sekunden eine negative Auswirkung auf die TCP-Verbindung. Negative Auswirkungen auf TCP für eine Dauer von 4 Sekunden nach einem Subnetzwechsel mit Mobile IP sind auch in [FS99] beschrieben. Eigene Messungen [FDZ99] haben negative Auswirkungen in einem Zeitraum von 3 Sekunden ergeben.

5.1.4 Zusammenfassung

Die Vermessungen des Schnellen Agent Discovery Verfahrens und des um das Fast Forwarding erweiterten Mobile IP Protokolls zeigen, daß sich mit Hilfe dieser Verfahren die Unterbrechungsdauern nach einem Subnetzwechsel eines mobilen Systems signifikant reduzieren lassen. Kommen beide Verfahren zum Einsatz, so kann innerhalb von ca. 25 ms nach dem Basisstationswechsel, der zugleich auch den Subnetzwechsel bedingt, die Konnektivität auf der Netzwerkschicht wiederhergestellt werden. Diese geringere Unterbrechungsdauer bedeutet hierbei zugleich auch eine geringere Anzahl an verlorenen Paketen. Von den kürzeren Unterbrechungen profitieren sowohl UDP-Datenströme als auch Ende-zu-Ende TCP-Datenströme.

5.2 Evaluation der Migrationskonzepte am Prototyp

Die in den vorangegangenen Abschnitten beschriebenen Messungen der prototypisch implementierten Konzepte belegen, daß mittels des Schnellen Agent Discoverys und des Fast Forwardings die durch Mobile IP bedingten Unterbrechungszeiten nach Subnetzwechseln signifikant reduziert werden können. Inwieweit allerdings der indirekte Transportansatz und hierbei insbesondere die Migration der Transportinstanzen Unterbrechungen zur Folge hat und inwieweit die Verfahren des in dieser Arbeit entwickelten OMIT-Konzeptes, d.h. die nebenläufige Migration (Kapitel 4.2.3) und die implizite Migration (Kapitel 4.4.2), zur Reduzierung dieser Unterbrechungsdauern geeignet sind, ist bisher nicht behandelt. Eine Beschreibung der anhand der Vermessung einer prototypischen Implementierung gewonnen Erkenntnisse erfolgt in diesem Kapitel. Eine Bewertung der Konzepte mittels simulativer Untersuchungen wird in Kapitel 5.3 vorgenommen. Die Vermessung der prototypischen Implementierung soll klären, inwieweit

- die nebenläufige Migration der Migration mit Einfrieren überlegen ist,
- die implizite der expliziten Migration überlegen ist,
- sich kurze, konstante Unterbrechungszeiten erzielen lassen und
- die nebenläufige Migration die Dauer der Migration verlängert.

5.2.1 Prototypische Implementierung

Gemeinsames Merkmal aller am Prototyp gemachten Untersuchungen ist die Realisierung der Migration der Statusinformation zum neuen Transportgateway über eine TCP-Verbindung. Da TCP einen zuverlässigen Übertragungsdienst zur Verfügung stellt, sind somit keine gesonderten Mechanismen im Migrationsagenten erforderlich, um die fehlerfreie Übertragung der Statusinformation zwischen den Transportgateways sicherzustellen.

Der Fokus der in diesem Kapitel beschriebenen Untersuchungen liegt auf der Bewertung der Migrationskonzepte. Sowohl die Mobile IP Erweiterungen Fast Forwarding und Schnelles Agent Discovery als auch die Mechanismen für automatische Basisstationswechsel sind im

vorangegangenen Kapitel untersucht worden und sind deshalb hier nicht Gegenstand der Betrachtungen. Ortswechsel und Basisstationswechsel werden seitens des mobilen Systems nicht vorgenommen. Stattdessen wird durch Eingriffe in das Routing gezielt dafür gesorgt, daß Pakete einer indirekten Transportverbindung jeweils über das aktuell als Transportgateway operierende System geroutet werden und darüber hinaus während der Phase der nebenläufigen Migration auch das passive Transportgateway passieren. Es erfolgt eine Nachbildung des Routings, wie es auch in Mobile IP zusammen mit dem Fast-Forwarding-Konzept realisiert ist. Die Unterbrechungsdauer nach Routenänderungen liegen mit ca. 10 ms in einer ähnlichen zeitlichen Größenordnung wie sie sich in Mobile IP, erweitert um das Schnelle Agent Discovery Konzept und das Fast-Forwarding-Konzept, realisieren lassen.

Implementierte Komponenten

Um mit vertretbarem Aufwand eine Bewertung der entwickelten Konzepte vornehmen zu können, wurde von einer Implementierung im Betriebssystemkern abgesehen. Die Implementierung erfolgt komplett im User-Space. Abb. 5.8 zeigt die Implementierungsarchitektur eines Transportgateways. Entlang schwarzer Linien werden Nutzdaten transportiert. Graue Linien sind im Kontext der Migration von Bedeutung. Entlang grauer, durchgezogener Linien wird die zu migrierende Statusinformation transportiert, graue gestrichelte Linien repräsentieren die Signalisierung. Auf die Funktion und die Interaktion der einzelnen Komponenten wird im folgenden eingegangen. Eine detailliertere Beschreibung der Architektur und der Implementierung ist in [Bö96] zu finden.

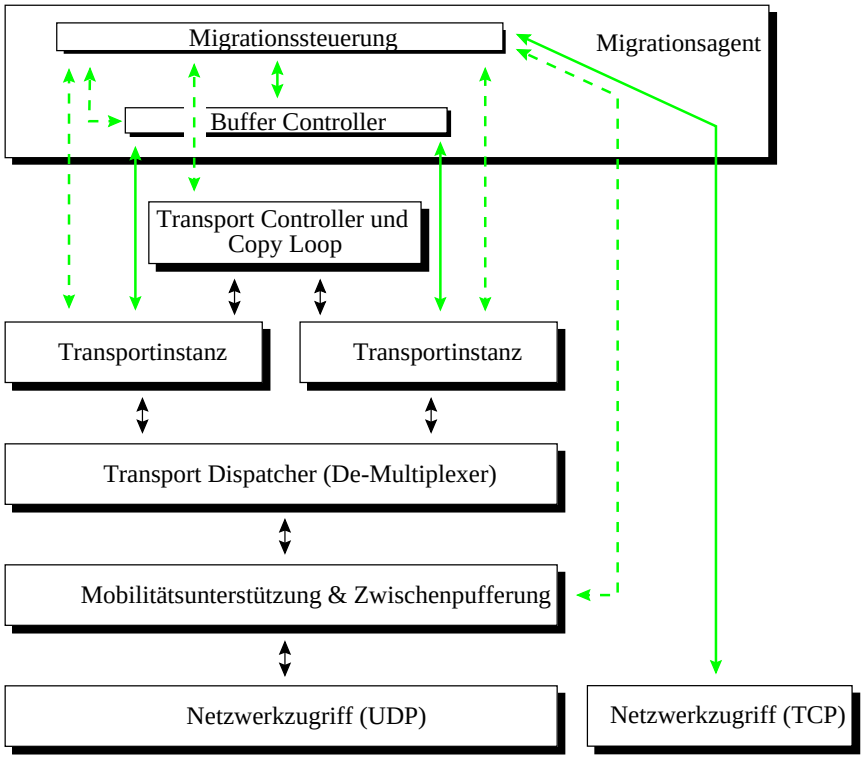


Abbildung 5.8: Architektur des Transportgateway Prototyps

Da das Transportprotokoll TCP im Kern der für die prototypische Implementierung eingesetzten Systeme realisiert ist, der im User-Space realisierte Migrationsagent aber Zugriff

auf die Pufferinhalte und die Protokollkontrollblöcke der Transportinstanzen benötigt, kann nicht auf dieser Protokollimplementierung des Kerns aufgesetzt werden. Stattdessen sind in der in Abb. 5.8 als Transportinstanz bezeichneten Komponente im User-Space die wesentlichen Mechanismen des Transportprotokolls TCP nachgebildet. Es sind dies timerbasierte Go-Back-N Übertragungswiederholungen, kumulative Bestätigungen und die Flußkontrolle. Sowohl die Mechanismen des Verbindungsaufbaus bzw. des Verbindungsabbaus als auch die Lastkontrolle wurden nicht in den Prototyp mit aufgenommen. Vollastszenarien haben schnelle und häufige Änderungen der zu migrierenden Pufferinhalte zur Folge. Sie erschweren somit die nebenläufige Migration und sind deshalb besonders untersuchenswert. Da die Realisierung von Lastkontrollmechanismen in der Transportinstanz langsamere Änderungen der Pufferinhalte zur Folge hätten, ist es für die Bewertung der Migrationskonzepte sinnvoll, auf ihre Realisierung in den Transportinstanzen des Prototyps zu verzichten.

Aufgabe des Transport Dispatchers ist es, anhand der Adressen und Portnummern zu entscheiden, an welche Transportinstanz ein Paket weiterzuleiten ist. In der Mobilitätsunterstützung wird Mobile IP erweitert um das Fast Forwarding nachgebildet. Auf Basis der Adressen und Portnummern wird bestimmt, an welche Komponente Pakete zur weiteren Bearbeitung übergeben werden. Pakete indirekter Transportverbindungen, für die das Zwischensystem als aktives Transportgateway fungiert, werden an den Dispatcher geliefert. Übernimmt das Transportgateway die Funktion eines passiven Transportgateways, so werden die Pakete an den Migrationsagent übergeben. Operiert das Zwischensystem nicht als Gateway, so erfolgt ein Mobile IP-Forwarding, d.h. die Komponente Netzwerkzugriff übernimmt die Weiterleitung der Pakete.

Der Transport Controller ist für die Instantiierung der zu einer Transportverbindung gehörenden Transportinstanzen verantwortlich. Darüber hinaus beinhaltet er die Copy Loop, die Pakete dem Sende- bzw. Empfangspuffer der einen Transportinstanz entnimmt und in den Empfangs- bzw. Sendepuffer der anderen Instanz kopiert. Der Transport Controller wird vom Migrationsagenten über die jeweilige, zu veranlassende Operation informiert.

Im Migrationsagent ist die Migrationssteuerung und der Buffer Controller realisiert. Der Buffer Controller hat Zugriff auf die Sende- und Empfangspuffer der beiden Transportinstanzen und ist darüber informiert, welche Puffer noch zu migrieren sind bzw. bereits migriert wurden. Im Buffer Controller wird die Entscheidung getroffen, welcher Puffer – in Abhängigkeit von der verwendeten Migrationsstrategie – als nächstes zu migrieren ist. Die Migrationssteuerung veranlaßt das Aktivieren und Einfrieren von Transportinstanzen, beauftragt den Buffer Controller mit der Selektion des nächsten zu migrierenden Puffers und übergibt die zu migrierenden Daten an TCP zur Übertragung zum neuen Transportgateway.

Abb. 5.9 zeigt zusätzlich zu den Komponenten der Systeme die den Messungen zu Grunde liegende Netztopologie. Das mobile System, der Festnetzrechner, der Home Agent, Transportgateway 1 und Transportgateway 2 sind an ein 100 Mbit/sec Ethernet Segment angeschlossen. Zusätzlich sind die beiden Transportgateways über ATM verbunden. Die Delays zwischen den dargestellten Rechnern liegen unterhalb von 1 ms. Die ATM-Strecke bietet den Vorteil einstellbarer Datenraten. Alle zwischen den beiden Transportgateways übertragenen Pakete werden über diese ATM-Strecke gesendet. Im Gegensatz zu den in [BB95a] beschriebenen Messungen, die von einer 10 Mbit/sec Ethernet Verbindung zwischen den Transportgateways ausgehen, können durch die gezielte Wahl der Bandbreite der ATM-Strecke zwischen den Transportgateways detailliertere Untersuchungen durchgeführt werden.

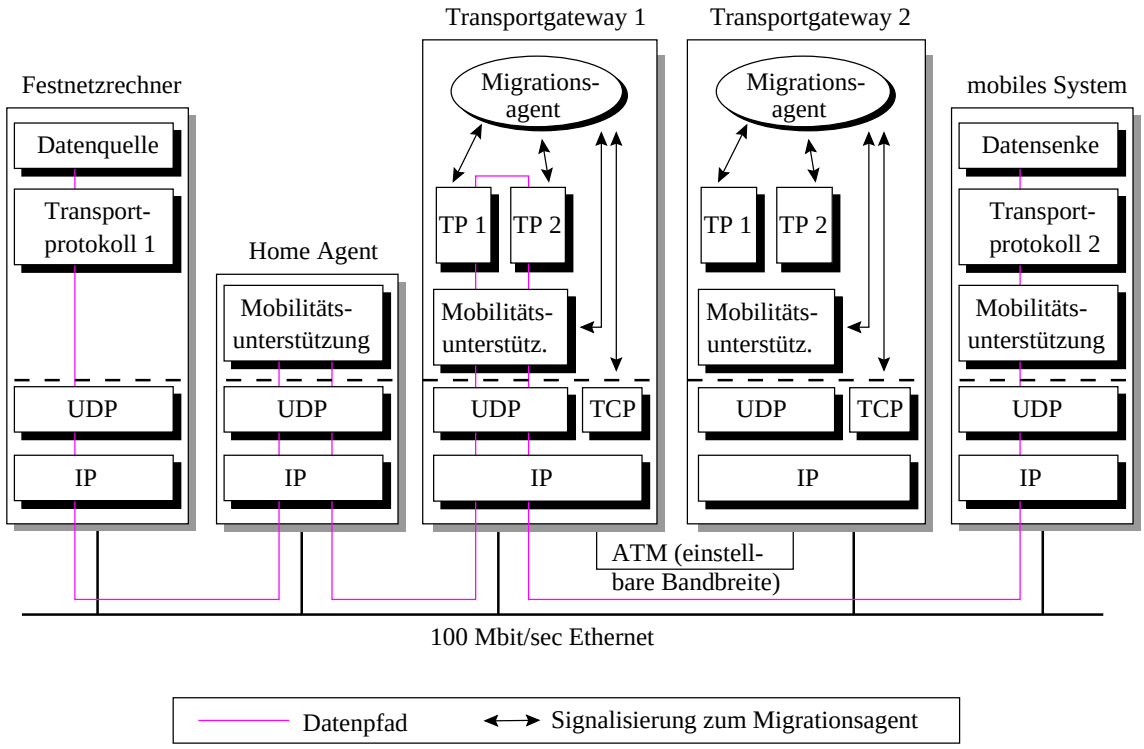


Abbildung 5.9: Konfiguration für die Untersuchungen am Prototyp

Die unterhalb der gestrichelten Linie dargestellten Komponenten sind im Kern des Betriebssystems angesiedelt. Auf Grund der Restriktion, Kernel Programmierung zu vermeiden, können sie zwar genutzt werden, aber keine Veränderungen an ihnen vorgenommen werden. Die dargestellte TCP-Instanz ist nicht zu verwechseln mit einer TCP-Instanz, die zu einer indirekten Transportverbindung gehört und durch die in diesem Kapitel untersuchten Mechanismen auf ein anderes Transportgateway migriert werden soll. Sie empfängt lediglich vom Migrationsagenten die zu migrierende Statusinformation und übergibt sie in dem neuen Transportgateway an den dortigen Migrationsagenten.

Über UDP werden die von den Transportinstanzen gesendeten Pakete übertragen. Die Mobilitätsunterstützung sorgt dafür, daß vom Festnetzrechner bzw. vom mobilen System gesendete Pakete zunächst zum aktiven Transportgateway übertragen werden. In Abb. 5.9 ist zusätzlich der Pfad der vom Festnetzrechner zum mobilen System gesendeten Pakete dargestellt. Sie passieren den Home Agent, werden im Transportgateway 1, das als aktives Gateway und Foreign Agent für das mobile System fungiert, in den Transportinstanzen bearbeitet und anschließend zum mobilen System gesendet. Vom mobilen System gesendete Pakete passieren ebenfalls das aktive Transportgateway, werden von diesem aber direkt, d.h. nicht über den Home Agent, zum Festnetzrechner weitergeleitet. Das Dreiecksrouting und die Weiterleitung gemäß der Mobile IP Erweiterung Fast Forwarding sind in der Mobilitätsunterstützung realisiert. Im Ausgangsszenario, d.h. vor der Migration, ist Transportgateway 2 nicht involviert. Im Fall einer Migration wird die Statusinformation zwischen Transportgateway 1 und Transportgateway 2 übertragen. Anschließend wird das Transportgateway 2 aktiviert und das Transportgateway 1 deaktiviert.

5.2.2 Grundlegendes Szenario der Messungen

Bedingt durch technologische Randbedingungen ist die über der drahtlosen Übertragungsstrecke verfügbare Übertragungsrate geringer als die im drahtgebundenen Backbone. Bei der Vermessung der prototypischen Implementierung wird dies mit berücksichtigt und nachgebildet, indem die zwischen dem Festnetzrechner und dem Transportgateway operierenden Transportverbindungen auf 100 KBytes/sec und die Transportverbindungen zwischen dem Transportgateway und dem mobilen System auf 50 KBytes/sec beschränkt werden. Dieser Unterschied bezüglich der verfügbaren Bandbreiten hat ggf. Warteschlangen im Transportgateway zur Folge.

Für Datenverkehr vom mobilen System zum Festnetzrechner bilden sich im Transportgateway keine bzw. allenfalls temporär Warteschlangen. Sendet hingegen der Festnetzrechner Daten an das mobile System, bilden sich im Transportgateway Warteschlangen auf Grund der geringeren auf der Strecke zwischen Transportgateway und dem mobilen System verfügbaren Bandbreite. Der Empfangspuffer der Partnertransportinstanz des Festnetzrechners und der Sendepuffer der Partnertransportinstanz des mobilen Systems bilden zusammen diese Warteschlange. Es füllt sich zunächst im Transportgateway der Sendepuffer der Partnertransportinstanz des mobilen Systems. Kann dieser keine weiteren Daten mehr aufnehmen, füllt sich im Transportgateway auch der Empfangspuffer der Partnertransportinstanz des Festnetzrechners. Da beide genannten Puffer der Transportinstanzen eine maximale Größe haben, ergibt sich auch für die Warteschlangenlänge eine Oberschranke. Pufferüberläufe werden von der Flußkontrolle des Transportprotokolls verhindert.

Die Dauer einer Migration hängt von der zur Verfügung stehenden Bandbreite und der Menge der Statusinformation ab, die vom alten auf das neue Transportgateway migriert werden muß. Diese Statusinformation umfaßt für jede der zwei zu migrierenden Transportinstanzen einen Empfangspuffer, einen Sendepuffer und einen Protokollkontrollblock. Die maximale Größe jedes dieser Puffer beträgt 32 KBytes. Für den Protokollkontrollblock wird eine Größe von 400 Bytes angenommen. Insgesamt ergeben sich somit maximal 64.8 KBytes zu migrierender Statusinformation. Da lediglich solche Szenarien, die gefüllte Puffer innerhalb der Transportinstanzen zur Folge haben, für die Bewertung der Migrationskonzepte interessant sind, ist in allen im folgenden untersuchten Szenarien der Sender auf dem Festnetzrechner realisiert. Die Datenquelle auf dem Festnetzrechner liefert ausreichend Daten, um den Sendepuffer der Transportinstanz sofort wieder zu füllen, nachdem, bedingt durch eine eintreffende Bestätigung, Platz verfügbar geworden ist. Beim untersuchten Szenario handelt es sich um ein Vollast-Szenario. Die Puffer der zu migrierenden Transportinstanzen sind zum Zeitpunkt der Migration komplett gefüllt.

Die Realisierbarkeit von Subnetzwechseln ohne nennenswerte Unterbrechung der Kommunikation in der Netzwerkschicht wurde bereits mittels der Vermessung der prototypischen Implementierung belegt. Kommt zusätzlich zu diesen Verfahren der indirekte Transportansatz zum Einsatz, so ergeben sich bedingt durch die Migration ggf. Unterbrechungen auf der Transportebene. Die Dauer dieser Unterbrechungen ist Gegenstand der im folgenden beschriebenen Untersuchungen.

Analog zu dem in Kapitel 5.1.3.2 diskutierten Szenario werden 5 Subnetzwechsel pro Minute, d.h. alle 12 Sekunden ein Subnetzwechsel, vorgenommen. Nach jedem Subnetzwechsel erfolgt eine Migration der Transportinstanzen auf das neue Transportgateway. Als Migrationsstrategie kommt die in [BB95a] vorgeschlagene *Migration mit Einfrieren* zum Einsatz. Da von

einer Puffergröße von 32 KBytes und 400 Bytes großen Protokollkontrollblöcken ausgegangen wird, sind bei jeder Migration 64.8 KBytes Statusinformation zum neuen Transportgateway zu übertragen. Während der Übertragung der Statusinformation ist die Transportverbindung unterbrochen.

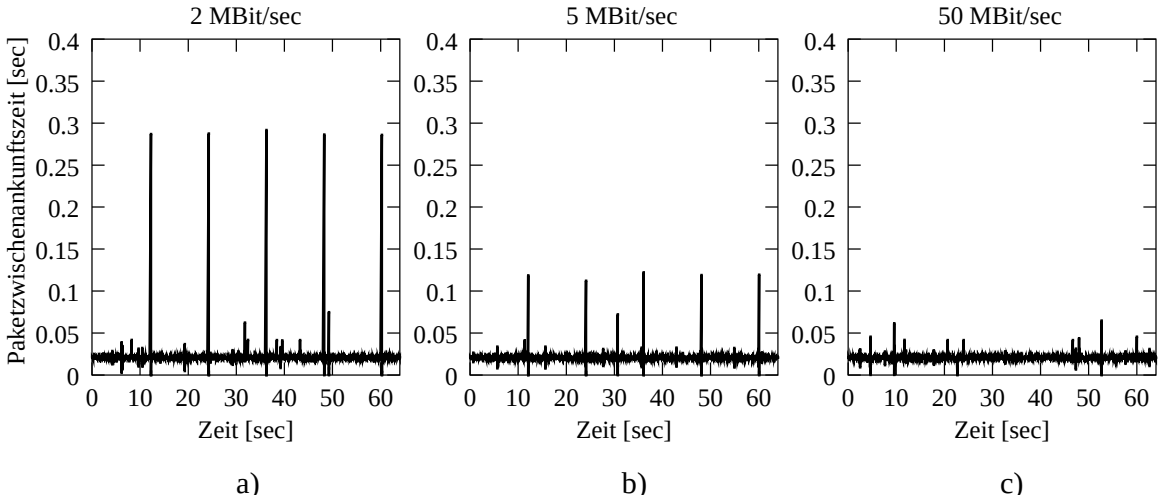


Abbildung 5.10: Unterbrechungsdauer: Migration mit Einfrieren

Die Dauer der Übertragung der Statusinformation zwischen dem alten und dem neuen Transportgateway hat direkten Einfluß auf die Dauer der Migration. Die Übertragungsdauer wiederum hängt von der zur Verfügung stehenden Bandbreite der die Transportgateways verbindenden Übertragungsstrecke und dem Hintergrundverkehr auf dieser Strecke ab.

Für maximale Übertragungsraten von 2 MBit/sec, 5 Mbit/sec bzw. 50 MBit/sec der Übertragungsstrecke zwischen den beiden Transportgateways des Prototyps zeigt Abb. 5.10 die Paketzwischenankunftszeiten zwischen einzelnen vom mobilen System empfangenen Paketen des Transportprotokolls. Hintergrundverkehr wird über diese Strecke nicht übertragen. Aus der Paketgröße von 1 KByte und der Übertragungsrate von 50 KBytes/sec ergibt sich eine Paketzwischenankunftszeit von 20 ms, die auch den Abbildungen entnommen werden kann. Zu den Zeitpunkten $12, 24, 36, 48$ und 60 erfolgt die Migration der Statusinformation zum neuen Transportgateway.

In Tabelle 5.2 sind die gemessenen, bzw. den Graphen entnehmbaren Unterbrechungsdauern und die rechnerisch für die Übertragung der Statusinformation erforderliche Zeit aufgeführt. Es handelt sich hierbei lediglich um eine Überschlagsrechnung, um die Korrektheit der Meßergebnisse zu untermauern.

	2 MBit/sec	5 MBit/sec	50 MBit/sec
Unterbrechungsdauer (Messung) [sec]	0.29	0.12	< 0.02
Übertragungsdauer (rechnerisch) [sec]	0.26	0.11	0.01

Tabelle 5.2: Gegenüberstellung: Meßergebnisse vs. Überschlagsrechnung

Die gemessenen Unterbrechungsdauern und die rechnerisch ermittelten Werte liegen in einer ähnlichen Größenordnung, d.h. die Korrektheit der Ergebnisse wird untermauert. Abweichende Ergebnisse sind hingegen in [BB95a] publiziert. Im dort beschriebenen Szenario

sind die beiden Transportgateways über ein 10 MBit/sec Ethernet verbunden. Als Übertragungsdauer für die Migration der Statusinformation werden 790 ms für die 32 KBytes Statusinformation der ersten Transportinstanz und 410 ms für die 32 KBytes Statusinformation der zweiten Transportinstanz angegeben. Als Ursache für die unterschiedlich lange Zeitdauer wird der Slow Start von TCP angeführt. Da das alte und das neue Transportgateway an demselben Ethernet Segment angeschlossen sind, sollte die Paketumlaufzeit zwischen den beiden Transportgateways sehr gering sein. Warum trotz einer geringen Paketumlaufzeit der Slow Start von TCP die Übertragung der 64 KBytes Statusinformation signifikant verzögert, wird von den Autoren nicht diskutiert. Die von den Autoren genannte Übertragungsdauer von 1200 ms über ein 10 MBit/sec Ethernet erscheint im Vergleich zu der durch eigene Messungen ermittelten und Überschlagsrechnungen bestätigten Übertragungsdauer von 260 ms über eine 2 Mbit/sec Strecke fragwürdig.

Die in Abb. 5.10c dargestellte Messung verdeutlicht, daß im Falle einer Übertragungsrate von 50 MBit/sec zwischen den beiden Transportgateways die Migration ohne erkennbare Unterbrechungen realisiert werden kann. In der Praxis werden allerdings sehr viele Datenströme über derartig breitbandige Übertragungsstrecken übertragen. Somit ist die für einen einzelnen Datenstrom verfügbare Bandbreite wesentlich geringer. Auch im Kontext der Migration von Statusinformation kann nicht davon ausgegangen werden, daß die Statusinformation mit einer Rate von mehreren 10 Mbit/sec zum neuen Transportgateway übertragen werden kann.

Zielsetzung muß es also sein, auch im Falle geringerer für die Migration der Statusinformation verfügbarer Übertragungsraten zwischen den Transportgateways die durch die Migration der Transportinstanzen verursachten Unterbrechungszeiten zu reduzieren. Für alle weiteren am Prototyp durchgeführten Untersuchungen wird von einer Übertragungsbandbreite von 2 Mbit/sec zwischen den beiden Transportgateways ausgegangen. Das im Rahmen dieser Arbeit entwickelte Konzept der nebenläufigen Migration – in den Varianten explizite bzw. implizite Migration – wird im folgenden hinsichtlich seiner Eignung bewertet, die durch die Migration der Transportinstanzen bedingten Unterbrechungszeiten zu reduzieren.

5.2.3 Nebenläufige explizite Migration vs. Migration mit Einfrieren

Die Migrationsdauer hängt direkt von der Menge der zu migrierenden Statusinformation ab. Diese wiederum ist durch den Füllungsgrad der Sende- bzw. Empfangspuffer der zu migrierenden Transportinstanzen bestimmt. Wegen der Abhängigkeit der Migrationsdauer vom Füllungsgrad der Puffer werden Meßreihen mit verschiedenen maximalen Puffergrößen (zwischen 2 KBytes und 32 KBytes) der Transportinstanzen durchgeführt. Für jede der untersuchten Puffergrößen wurden 80 Meßläufe durchgeführt und für die Migrationsdauer bzw. die Dauer der Unterbrechung das arithmetische Mittel aus den einzelnen gemessenen Werten bestimmt. Gestartet wurde die Migration jeweils unmittelbar nach dem Subnetzwechsel.

Für die Bewertung relevante Zeitpunkte sind der Zeitpunkt des Einfrierens der Transportinstanzen auf dem alten Transportgateway und der Zeitpunkt des Aktivierens der Transportinstanzen auf dem neuen Transportgateway. Beide Zeitpunkte werden relativ zum Zeitpunkt des Starts der Migration bestimmt. Als *Migrationsdauer* wird die Zeitdauer vom Start der Migration bis zum Aktivieren der Transportinstanzen auf dem neuen Transportgateway bezeichnet. Die *Unterbrechungsdauer* ist bestimmt durch die Zeit, die vom Deaktivieren des

alten Transportgateways bis zum Aktivieren des neuen Transportgateways vergeht.

5.2.3.1 Migrationsdauer

Abb. 5.11 können die Migrationsdauern für die Migration mit Einfrieren und die nebenläufige Migration entnommen werden. Die nebenläufige Migration erfolgt durch explizite Übertragung der Puffer, d.h. es kommt die Variante explizite Migration zum Einsatz. Auf der x-Achse ist die maximale Größe eines einzelnen Sende- bzw. Empfangspuffers aufgetragen. Da im betrachteten Szenario ein Sendepuffer und ein Empfangspuffer zu migrieren sind, beträgt die Menge der zum neuen Transportgateway zu übertragenden Statusinformation das doppelte des auf der x-Achse aufgetragenen Wertes.

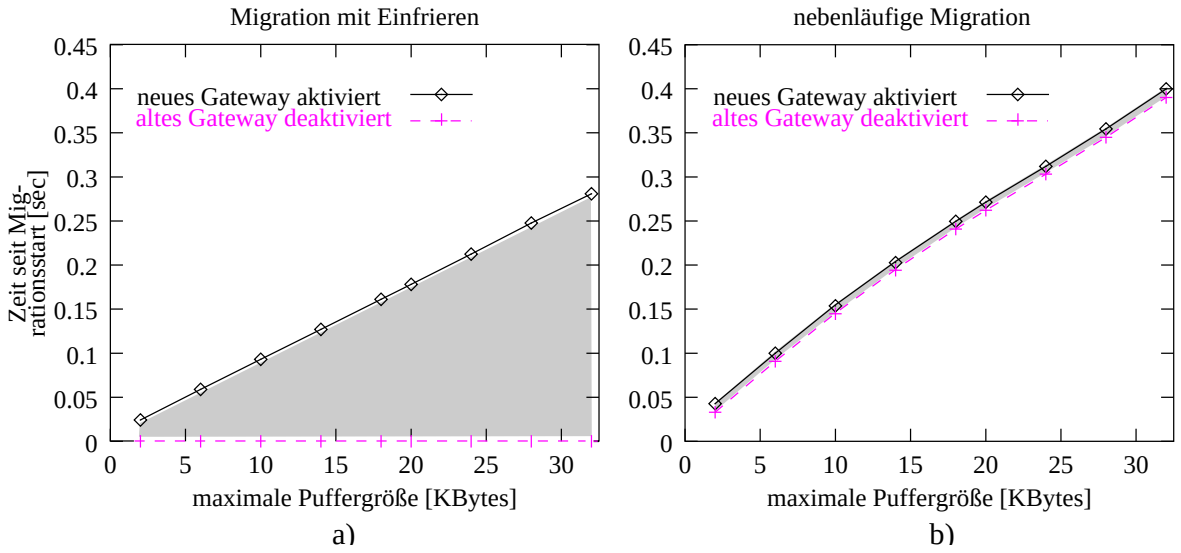


Abbildung 5.11: Dauer der Migration mit Einfrieren bzw. der nebenläufigen Migration

Erwartungsgemäß steigt die Migrationsdauer sowohl für die Migration mit Einfrieren als auch für die nebenläufige Migration linear mit der maximalen Puffergröße an. Für die Migration mit Einfrieren ergibt sich für eine Puffergröße von 32 KBytes, d.h. 64 KBytes migrierter Pufferinhalte, im Mittel eine Unterbrechungsdauer von ca. 0.28 sec. Die in Abb. 5.10a dargestellten Paketzwischenankunftszeiten zum Zeitpunkt der Migration liegen mit 0.29 sec in einer ähnlichen Größenordnung.

Bei der Migration mit Einfrieren erfolgt die Deaktivierung des alten Transportgateways unmittelbar nach dem Migrationsstart. Die gepunktete Linie, die in Abb. 5.11a direkt auf der x-Achse liegt, bringt dies zum Ausdruck. Der grau dargestellte Bereich reflektiert die Unterbrechungsdauer. Deutlich zu erkennen ist, daß die Unterbrechungsdauer linear mit der Menge der zu migrierenden Puffer bis auf 0.28 sec anwächst.

Abb. 5.11b zeigt die Situation für die nebenläufige Migration. Da das alte Transportgateway erst eingefroren wird, nachdem die Statusinformation komplett migriert wurde, ist der Zeitpunkt des Einfrierens abhängig von der Menge der zu migrierenden Daten. Der Einfrierzeitpunkt steigt linear mit der Menge der zu migrierenden Daten. Die grau dargestellte Unterbrechungsdauer ist hingegen konstant und wächst nicht mit der Menge der migrierten

Statusinformation. Im Vergleich zur Migration mit Einfrieren dauert die nebenläufige Migration länger. Ursache ist die auch während der Übertragung der Statusinformation weiterhin aktive Kommunikation auf der Transportebene.

In Abb. 5.11 ist lediglich die über 80 Meßläufe gemittelte Migrationsdauer dargestellt. Die in Tabelle 5.3 sowohl für die Migration mit Einfrieren als auch für die nebenläufige Migration aufgeführte Standardabweichung verdeutlicht die geringen Schwankungen der gemessenen Werte.

max. Puffergröße	2	6	10	14	18	20	24	28	32
Migration mit Einfrieren [sec]	0.001	0.004	0.002	0.003	0.001	0.001	0.001	0.003	0.001
nebenläufige Migration [sec]	0.001	0.006	0.006	0.005	0.004	0.004	0.004	0.003	0.005

Tabelle 5.3: Standardabweichungen der Migrationsdauern

Für die Migration mit Einfrieren und eine Puffergröße von 32 KBytes wurde die im Mittel gemessene Migrationsdauer von 0.28 sec bereits in Kapitel 5.2.2 durch eine Überschlagsrechnung bestätigt. Um auch für die nebenläufige Migration die gemessenen Migrationsdauer von 0.40 sec zu bestätigen, wird auch für diese Migrationsstrategie eine derartige Berechnung durchgeführt.

Bedingt durch das Fast Forwarding werden die vom aktiven Transportgateway zum mobilen System übertragenen Transportprotokolldateneinheiten über die 2 Mbit/sec ATM-Strecke übertragen. 50 KBytes/sec, d.h. 400 Kbit/sec, der 2 Mbit/sec Bandbreite sind hierfür erforderlich. Für die Migration der Statusinformation stehen somit lediglich 1.6 Mbit/sec zur Verfügung.

	Migrierte Puffer [KBytes]	Übertragungsdauer [sec]	währenddessen neu empfangene TPDU's
Phase 1	64	0.32	16
Phase 2	16	0.08	4
Phase 3	4	0.02	0
Summe	84	**0.42**	20

Tabelle 5.4: Nebenläufige Migration: Überschlägige Bestimmung der Migrationsdauer

Die während der einzelnen Phasen migrierte Menge an Statusinformation und die hierfür erforderlichen Zeiten sind in Tabelle 5.4 aufgeführt. Zu Beginn der Migration sind der jeweils 32 KBytes große Empfangspuffer und Sendepuffer gefüllt. Für ihre Migration zum neuen Transportgateway steht wie bereits beschrieben eine Bandbreite von 1.6 Mbit/sec zur Verfügung. Es ergibt sich somit eine Übertragungszeit von 0.32 sec. Während dieser Zeitdauer ist die Transportkommunikation weiterhin aktiv. Da das aktive Transportgateway alle 20 ms ein weiteres 1 KBytes großes Paket der Partnertransportinstanz empfängt, werden während der genannten 0.32 sec weitere 16 KBytes Daten zum Transportgateway übertragen. Diese Pufferinhalte werden in der zweiten Phase der Migration zum neuen Transportgateway migriert. Während der hierfür erforderlichen 0.08 sec werden vom Transportgateway 4 weitere Pakete der Transportinstanz empfangen. Diese werden in der dritten Phase der Migration

zum neuen Transportgateway gesendet. Aufsummiert ergibt sich eine Migrationsdauer von 0.42 sec. Diese rechnerisch ermittelte Zeitdauer liegt in einer ähnlichen Größenordnung wie die gemessenen 0.40 sec und bestätigt somit den gemessenen Wert.

5.2.3.2 Unterbrechungsdauer

Bei der Beschreibung des Konzeptes der nebenläufigen Migration wurden kurze und konstante, d.h. von der Menge der zu migrierenden Statusinformation unabhängige Unterbrechungsdauern als herausragendes Merkmal herausgestellt. Inwieweit sich diese Zielsetzungen erreichen lassen, kann Abb. 5.12 entnommen werden. Den Messungen liegt das im vorangegangenen Kapitel bereits beschriebene Szenario zu Grunde.

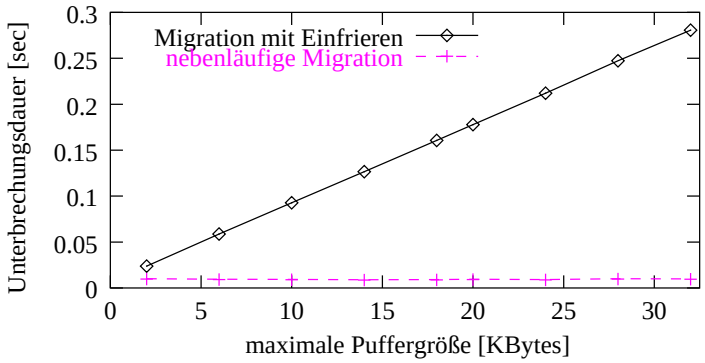


Abbildung 5.12: Unterbrechungen: nebenläufige Migration vs. Migration mit Einfrieren

Gemittelt über die Meßläufe ergibt sich für die nebenläufige Migration eine konstante Unterbrechungsdauer von ca. 10 ms. Bei der Migration mit Einfrieren steigt sie hingegen bis auf 0.28 sec an. Für eine Bewertung ist es allerdings nicht ausreichend, lediglich die im Mittel erzielbaren Unterbrechungszeiten zu betrachten. Es interessieren vielmehr auch die sich maximal ergebenden Unterbrechungsdauern. Bei der im nächsten Kapitel beschriebenen vergleichenden Bewertung der impliziten und expliziten Migration wird zusätzlich auf die sich maximal ergebenden Unterbrechungsdauern eingegangen.

5.2.4 Implizite vs. explizite Migration

Der Nutzen der nebenläufigen Migration im Vergleich zur Migration mit Einfrieren wurde am Beispiel der expliziten Migration in den beschriebenen Untersuchungen nachgewiesen. Inwieweit sich für die implizite bzw. die explizite Migration verschiedene Ergebnisse ergeben, wird im folgenden diskutiert.

5.2.4.1 Migrationsdauer

Bei der expliziten Migration werden alle Pufferinhalte durch eine gesonderte Übertragung (siehe Kapitel 4.4.2.3) migriert. Bei der impliziten Migration erlangt hingegen das neue Transportgateway von einem Teil der zu migrierenden Pufferinhalte durch Mitlauschen, d.h. implizit Kenntnis, lediglich den verbleibenden Teil empfängt es durch eine gesonderte Übertragung. Die geringere Menge durch gesonderte Übertragung migrierter Statusinformation im Falle der

impliziten Migration läßt eigentlich eine geringere Migrationsdauer erwarten. Da die Messungen wider Erwarten keinen signifikanten Unterschied zwischen der impliziten und der expliziten Migration bzgl. der Migrationsdauer ergaben, ist die Migrationsdauer für die implizite Migration nicht in einem weiteren Graphen dargestellt (Abb. 5.11b). Eine Analyse der Menge der gesondert übertragenen Statusinformation ergab für beide Varianten nahezu identische Werte, d.h. die implizite Migration konnte nicht von durch Mitlauschen migrierten Puffern profitieren.

Pakete, die während der Migration implizit zum neuen, passiven Transportgateway übertragen werden, werden im neuen Transportgateway als Kopie an die dortige, noch inaktive Transportinstanz übergeben. Da auf Grund der kurzen Paketumlaufzeit von ca. 1 ms aber bereits kurze Zeit später das von der Transportschicht des mobilen Systems generierte Bestätigungspaket beim alten, aktiven Transportgateway eintrifft, entfernt das aktive Transportgateway das Paket aus dem Sendepuffer. Das Paket gehört somit nicht mehr zur Menge der zu migrierenden Statusinformation. Die zuvor implizite Migration des Pakets zum neuen Transportgateway hat aus diesem Grunde keinen Nutzen.

Wesentliche Ursache für den geringen Nutzen der impliziten Migration ist ein geringe Paketumlaufzeit zwischen dem aktiven Transportgateway und dem mobilen System. Warteschlangen in Zwischensystemen oder längere Signallaufzeiten können eine größere Paketumlaufzeit zur Folge haben. Inwieweit in einem derartigen Szenario die implizite der expliziten Migration überlegen ist, wird in den in Kapitel 5.3 beschriebenen simulativen Untersuchungen betrachtet.

5.2.4.2 Unterbrechungsdauer

Das Konzept der nebenläufigen Migration wurde mit dem Anspruch entwickelt, kurze und konstante, von der Menge der zu migrierenden Statusinformation unabhängige Unterbrechungszeiten zu realisieren. Daß die nebenläufige Migration im Vergleich zur Migration mit Einfrieren kurze Unterbrechungen ermöglicht, wurde bereits anhand von Abb. 5.12 verdeutlicht. Bedingt durch die Skalierung dieser Abbildung ist nicht zu erkennen, inwieweit die Unterbrechungsdauer auch konstant, d.h. unabhängig von der Menge der zu migrierenden Statusinformation ist.

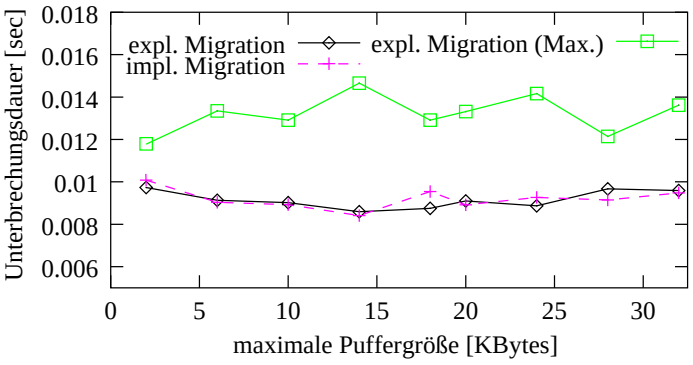


Abbildung 5.13: Unterbrechungsdauer: implizite vs. explizite Migration

Abb. 5.13 zeigt die über 80 Meßläufe gemittelte Unterbrechungsdauer für die implizite und die explizite Migration. Deutlich zu erkennen ist die nahezu konstante Unterbrechungsdauer

von ca. 10 ms. Hinsichtlich der Unterbrechungsdauer unterscheiden sich die beiden Varianten der nebenläufigen Migration nicht signifikant. Zusätzlich zu den gemittelten Unterbrechungsdauern sind für die explizite Migration die Maximalwerte der Unterbrechungsdauern mit in die Abbildung aufgenommen. Für keine der untersuchten Puffergrößen dauert die durch eine Migration bedingte Unterbrechung der Transportkommunikation länger als 15 ms.

5.2.5 Zusammenfassung der Meßergebnisse

Die Vermessung der Prototypen belegt, daß der Einsatz des indirekten Transportansatzes nicht zwangsläufig signifikante Unterbrechungen der Transportkommunikation im Falle der Migration zur Folge haben muß. Mittels der nebenläufigen Migration lassen sich die durch die Migration bedingten Unterbrechungszeiten auf im Mittel ca. 10 ms reduzieren. Im untersuchten Szenario hatte keine der im Zuge der Meßreihen vorgenommenen 720 Migrationen eine Unterbrechung der Transportkommunikation von mehr als 15 ms zur Folge.

Einen Nachweis kürzerer Migrationsdauern im Falle der impliziten Migration im Vergleich zur expliziten Migration liefert die Vermessung des Prototyps nicht. Als ursächlich hierfür erwies sich die durch das gewählte Szenario bedingte kurze Paketumlaufzeit von ca. 1 ms zwischen dem aktiven Transportgateway und dem mobilen System. Inwieweit im Falle einer längeren Paketumlaufzeit zwischen aktivem Transportgateway und mobilem System die implizite Migration der expliziten Migration überlegen ist, wird unter anderem in den im nächsten Kapitel beschrieben simulativen Untersuchungen betrachtet.

5.3 Evaluation der Migrationskonzepte durch Simulation

Um weitergehende Betrachtungen anstellen zu können und um darüber hinaus sicherzustellen, daß die Meßergebnisse nicht die Folge implementierungsspezifischer Details der prototypischen Implementierung sind, sind zusätzlich auch simulative Untersuchungen durchgeführt worden. Während den am Prototyp durchgeführten Messungen ein Vollastszenario zugrundelag, werden bei den simulativen Untersuchungen darüber hinausgehend auch Teillastszenarien betrachtet. Weiterhin wird diskutiert, inwieweit die implizite Migration der expliziten Migration im Falle einer in der Größenordnung von 100 ms liegenden Paketumlaufzeit zwischen dem Transportgateway und dem mobilen System überlegen ist. Darüber hinaus wird auch ein anderer *Migrationszeitpunkt* gewählt. Abweichend von den am Prototyp vorgenommenen Untersuchungen erfolgt die Migration nicht sofort nach dem Subnetzwechsel, sondern zu einem späteren Zeitpunkt. Mittels Fast Forwarding wird zunächst die Konnektivität in der Schicht 3 wiederhergestellt und erst danach zu einem späteren Zeitpunkt die Migration vorgenommen.

5.3.1 Simulationswerkzeug

Für die Simulationen wurde das Simulationswerkzeug Sim PlusPlus [Ros92a] eingesetzt. Das Tool ist in der Programmiersprache C++ realisiert und erweitert diese um Konstrukte, die eine prozeßorientierte Simulation zeitdiskreter Ereignisse ermöglichen. Die Unterstützung des prozeßorientierten Ansatzes erfolgt in Form eines Koroutinen-Konzeptes, das in C++ nicht

verfügbar ist. Da es sich bei der Nebenläufigkeit um ein in C++ nicht vorhandenes Konstrukt zur Steuerung des Kontrollflusses handelt, erfordert die Erstellung eines Simulationsmodells mittels Sim PlusPlus ein Umdenken seitens des Programmierers. Wesentlicher Vorteil des prozeßorientierten Ansatzes ist, daß die im Modell nachgebildeten logischen Zusammenhänge einzelner Aktivitäten leichter im Programmcode nachzuvollziehen sind als beim ereignisorientierten Ansatz. Dies erleichtert insbesondere, die Modellierung von Komponenten durch Studium des ggf. fremden Quellkodes nachzuvollziehen.

Die Erweiterung SimEnv [Ros92b] für Sim PlusPlus bietet eine speziell auf die Simulation von Netzwerken zugeschnittene Umgebung. Analog zum OSI-Referenzmodell wird im Simulationsmodell ein Netzwerkknoten aus mehreren, direkt miteinander kommunizierenden Schichten zusammengesetzt. Mittels einer speziellen Beschreibungssprache wird das zu untersuchende Szenario definiert. Es können die zu untersuchenden Netztopologien, Parameterwerte einzelner Variablen und der Detaillierungsgrad der zu sammelnden Simulationsdaten in der Beschreibungssprache festgelegt werden. Ohne den Programmcode des Simulationsmodells ändern zu müssen, können verschiedene Szenarien untersucht werden. Insbesondere ermöglicht die Beschreibungssprache, automatisierte Simulationsläufe für verschiedene Werte eines Parameters durchzuführen.

Eine graphische Visualisierung der Vorgänge innerhalb des Simulationsmodells bietet weder Sim PlusPlus noch SimEnv. Für die Visualisierung der zwischen den einzelnen modellierten Schichten eines Netzwerkknotens ausgetauschten Pakete wurde deshalb ein weiteres Werkzeug [Mad97] entwickelt. Eine kurze Beschreibung des Werkzeuges und der ihm zugrundeliegenden Ideen ist in Anhang B zu finden.

5.3.2 Simulationsmodell und simulierte Netztopologie

Die Netztopologie und die modellierten Schichten der beteiligten Systeme sind in Abb. 5.14 dargestellt. Hellgrau unterlegte Schichten werden von der Simulationsumgebung zur Verfügung gestellt. Modelle für die dunkelgrau dargestellten Schichten mußten für die Untersuchungen der Migrationsstrategien neu erstellt werden. Eine über die folgenden Ausführungen hinausgehende Beschreibung des simulierten Szenarios ist in [Str99] zu finden.

In der simulierten Konfiguration sind die Systeme durch Duplex Leitungen mit einstellbarer Datenrate und einstellbarem Delay verbunden. Eine Modellierung von Übertragungsfehlern auf diesen Leitungen ist nicht realisiert. Die Leitungen zwischen den Basisstationen und dem mobilen System bieten eine Übertragungsrate von 2 MBit/sec. Die Übertragungsrate zwischen den beiden Transportgateways variiert bei den verschiedenen durchgeführten Untersuchungen. Alle übrigen Leitungen haben eine Rate von 100 Mbit/sec. Warteschlangen, die sich auf Grund der unterschiedlichen Übertragungsraten der bei den Basisstationen eintreffenden Leitungen bilden können, sind im Modell berücksichtigt.

Da auf Duplex Punkt-zu-Punkt Leitungen keine Mechanismen zur Koordination des Medienzugriffs erforderlich sind und darüber hinaus in der Schicht 2 keine speziellen Protokollmechanismen zum Einsatz kommen, ist die Modellierung der als „Schicht 2 & physikalischer Zugriff“ bezeichneten Schicht von geringer Komplexität. In ihr ist, abgesehen von der Übergabe der Pakete zwischen der Netzwerkschicht und den Leitungsenden, keine weitere Funktionalität modelliert. Im Modell der Netzwerkschicht werden Routingentscheidungen auf Basis des Shortest-Path-Routings getroffen.

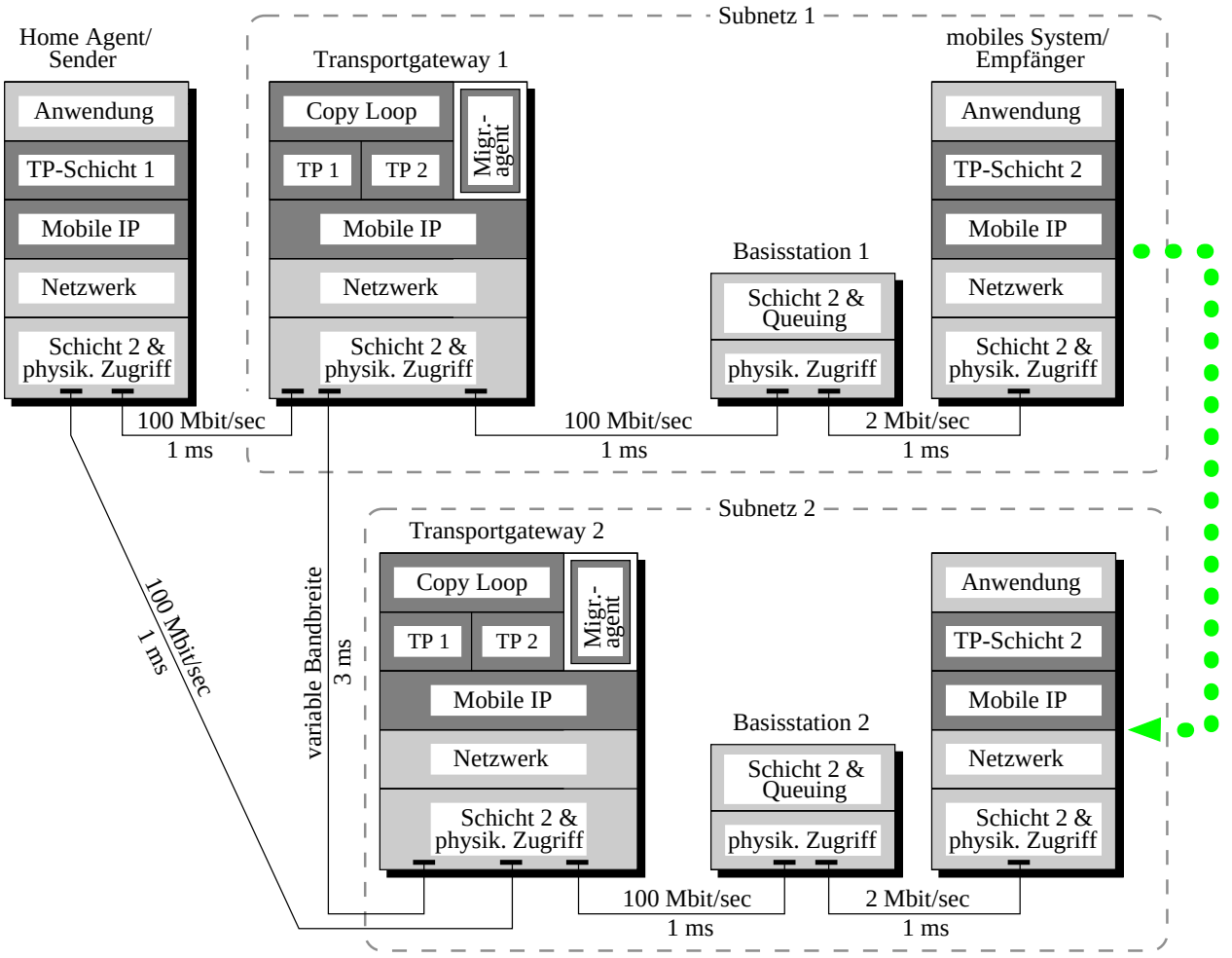


Abbildung 5.14: Konfiguration für die simulativen Untersuchungen

Die Übertragung der Pakete an das jeweils aktive Transportgateway und – im Falle des Fast Forwardings – das ggf. erforderliche Weiterleiten der Pakete zum passiven Transportgateway ist in der Mobile IP Schicht modelliert. Hierfür wird ein Tunnelmechanismus eingesetzt. Mobile IP Nachrichten werden im Modell nicht ausgetauscht, stattdessen werden mittels der Beschreibungssprache der Simulationsumgebung SimEnv zum Zeitpunkt eines Subnetzwechsels der Home Agent, die Transportgateways und das mobile System über den Subnetzwechsel informiert. Innerhalb der Modellierung der Mobile IP Schicht kann mittels dieser Information entschieden werden, ob und an welches System Pakete zu tunneln sind. Um zusätzliche Komplexität des Simulationsmodells zu vermeiden, ist der Dispatcher nicht in einer eigenen Schicht nachgebildet, sondern in die Mobile IP Schicht integriert. Er entscheidet, ob Pakete an den Migrationsagenten weiterzuleiten sind bzw. an welche Transportinstanz sie zu übergeben sind.

Zwischen dem Home Agent und dem Transportgateway wird das gleiche Transportprotokoll eingesetzt wie zwischen dem Transportgateway und dem mobilen System. Das modellierte Transportprotokoll umfaßt selektive Bestätigungen, selektive Übertragungswiederholungen auf Grund von Statusinformation, timerbasierte Übertragungswiederholungen sowie eine fensterbasierte Flußkontrolle, aber keine Lastkontrolle. Da der Fokus der Untersuchungen auf der Bewertung der Migrationsstrategien liegt und aus diesem Grund Übertragungsfehler auf den

Übertragungsstrecken nicht mit in das Modell integriert sind, sind die im Transportprotokoll modellierten Mechanismen der Fehlererkennung und Fehlerkorrektur nicht von wesentlicher Bedeutung. Deshalb ist es auch nicht problematisch, daß in dem Transportprotokoll zwischen dem Home Agent und dem Transportgateway nicht die Protokollmechanismen von TCP, sondern die oben aufgeführten Mechanismen modelliert sind. Bezüglich der Entscheidung, keine Lastkontrollmechanismen in das Modell mit aufzunehmen gelten die Aussagen, die bereits bei der Beschreibung der prototypischen Implementierung (siehe Seite 152) als Motivation für den Verzicht auf Lastkontrollmechanismen angeführt wurden.

Die Konzepte der Migration mit Einfrieren bzw. der nebenläufigen Migration, die im Rahmen dieser Arbeit betrachtet werden, sind im Migrationsagenten detailgetreu modelliert. Die Modellierung umfaßt sowohl die implizite als auch die explizite Migration unter Berücksichtigung der vorgestellten Pufferauswahlstrategie. Für den Austausch der Nutzdaten zwischen den Transportinstanzen in einem Transportgateway ist die Copy Loop verantwortlich.

5.3.3 Migration mittels unzuverlässiger Transportdienste

Bei der prototypischen Implementierung erfolgte die Übertragung der zu migrierenden Statusinformation zwischen den Migrationsagenten über TCP, d.h. mittels eines zuverlässigen Übertragungsdienstes. Im Simulationsmodell nutzt der Migrationsagent hingegen einen unzuverlässigen Übertragungsdienst, um die zu migrierende Statusinformation zum neuen Transportgateway zu senden. Da im Modell keine Übertragungsfehler modelliert sind, macht es keinen wesentlichen Unterschied, ob ein unzuverlässiger Übertragungsdienst zusammen mit speziellen im Migrationsagenten implementierten Mechanismen, die einen zuverlässigen Austausch der Statusinformation sicherstellen, oder ein zuverlässiger Übertragungsdienst verwendet wird. Das alte Transportgateway wird mittels Kontrollinformation vom neuen Transportgateway über bereits erfolgreich migrierte Puffer informiert und kann somit entscheiden, welche Pufferinhalte noch zu migrieren sind.

Es wird darüber hinaus davon ausgegangen, daß die Übertragung der Statusinformation zwischen dem alten Transportgateway und dem neuen Transportgateway drahtgebunden erfolgt. Auswirkungen von Übertragungsfehlern zwischen dem alten und dem neuen Transportgateway sind aus diesem Grunde nicht Gegenstand der Betrachtungen. Da zwischen den Transportgateways eine fehlerfreie Übertragungsstrecke modelliert ist, sollten sich, obwohl bei den simulativen Untersuchungen die Pufferinhalte über einen unzuverlässigen Transportdienst migriert werden, keine signifikanten Unterschiede hinsichtlich der Migrationsdauer und der Unterbrechungsdauer der Transportverbindungen zu den am Prototyp vorgenommenen Messungen ergeben.

Für die Migration mit Einfrieren sind in Abb. 5.15 die sich jeweils durch Mittelwertbildung aus 30 Simulationsläufen ergebenden Unterbrechungsdauern aufgeführt. In Abb. 5.15a ist die Unterbrechungsdauer in Abhängigkeit von der maximalen Puffergröße dargestellt. Die Datenrate des Links zwischen den beiden Transportgateways beträgt 2 Mbit/sec. Eine lineare Abhängigkeit, die auch schon die Vermessung des Prototypen ergeben hat, ist deutlich zu erkennen. Die sich bei einer maximalen Puffergröße von 2*32 KBytes ergebende Unterbrechungsdauer von ca. 0.26 sec liegt in einer ähnlichen Größenordnung wie die am Prototyp gemessene Unterbrechungsdauer von ca. 0.28 sec (siehe Abb. 5.12). Da die simulativen Untersuchungen und die Vermessung des Prototyps ähnliche Ergebnisse liefern, kann davon aus-

gegangen werden, daß weder implementierungsspezifische Details noch Unzulänglichkeiten in der Modellierung diese Ergebnisse entscheidend geprägt haben.

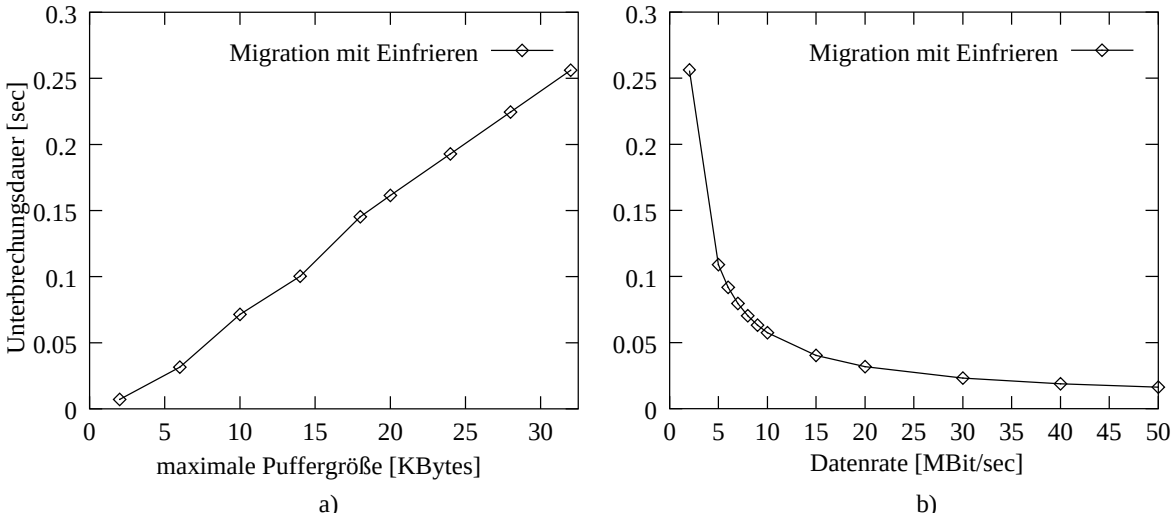


Abbildung 5.15: Unterbrechungsdauer: Migration mit Einfrieren

Abb. 5.15b zeigt, inwieweit die für die Migration der Daten verfügbare Bandbreite Einfluß auf die Dauer der Unterbrechung hat. Die maximale Puffergröße ist konstant und beträgt im betrachteten Szenario 32 KBytes. Für eine Datenrate von 2 Mbit/sec ergibt sich die auch Abb. 5.15a entnehmbare Unterbrechungsdauer von ca. 0.26 sec. Mit wachsender zur Verfügung stehender Bandbreite fällt die Unterbrechungsdauer erwartungsgemäß proportional zu $\frac{2 * 32000 * 8}{Datenrate}$.

Inwieweit im Falle der nebenläufigen Migration die maximale Puffergröße bzw. die zwischen den beiden Transportgateways für die Migration zur Verfügung stehende Bandbreite Einfluß auf die Unterbrechungsdauer hat, kann Abb. 5.16 entnommen werden. Für eine maximale Übertragungsrate von 6 Mbit/sec zwischen den beiden Transportgateways ergeben sich die in Abb. 5.16a dargestellten gemittelten Unterbrechungsdauern. Der Mittelwert liegt konstant bei ca. 6 ms. Eine Analyse der Einzelwerte ergab einen Maximalwert von 9 ms. Die Realisierbarkeit konstanter Unterbrechungsdauern unabhängig von der verfügbaren Bandbreite belegt Abb. 5.16b.

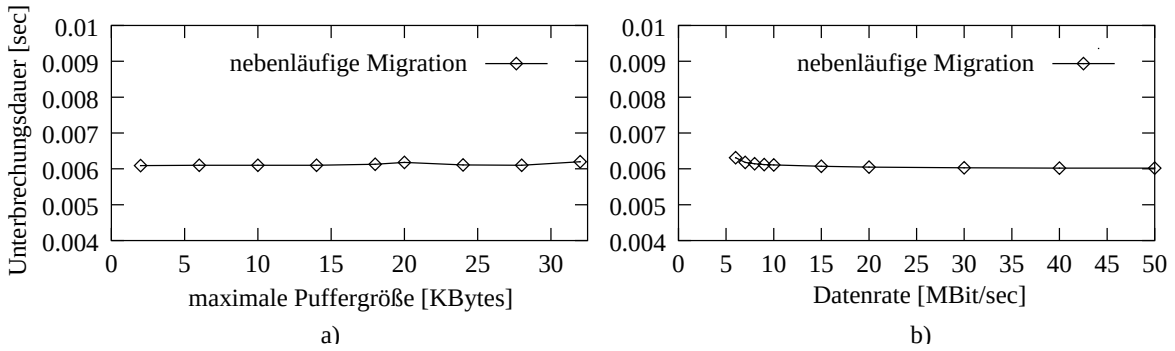


Abbildung 5.16: Unterbrechungsdauer: nebenläufige Migration

Den in Abb. 5.15a und Abb. 5.16a dargestellten Simulationsergebnissen liegen Szenarien zugrunde, die bereits durch Vermessung der Prototyps untersucht wurden. Die Tatsache, daß

sowohl die Vermessung der Prototyps als auch die simulativen Untersuchungen zu identischen Ergebnissen führen, untermauert die Korrektheit dieser Ergebnisse. Darüber hinausgehende Ergebnisse, die nicht bereits durch die Vermessung des Prototyps erlangt wurden, liefert die simulative Untersuchung des Einflusses der zwischen den beiden Transportgateways für die Migration verfügbaren Bandbreite. Abb. 5.16b verdeutlicht die Realisierbarkeit kurzer, konstanter Unterbrechungszeiten auch im Falle geringer verfügbarer Bandbreiten. Für Datenraten von weniger als 6 MBit/sec zwischen den beiden Transportgateways ist keine Unterbrechungsdauer aufgeführt, da im untersuchten Szenario bei der nebenläufigen, expliziten Migration minimal eine Bandbreite von 6 Mbit/sec zwischen den Transportgateways zur Verfügung stehen muß. Auf diesen Aspekt wird im nachfolgenden Unterkapitel genauer eingegangen.

5.3.4 Vollast vs. Teillast

Veränderungen der Pufferinhalte der zu migrierenden Transportinstanzen haben direkten Einfluß auf die Dauer der nebenläufigen Migration. Die Geschwindigkeit und die Häufigkeit der Pufferänderungen hängen ihrerseits vom Eintreffen von Transportprotokollpaketen ab. Da schnelle und häufige Änderungen der Statusinformation die nebenläufige Migration erschweren und längere Migrationsdauern zur Folge haben, sind derartige Szenarien besonders untersuchenswert.

Im folgenden wird die Migrationsdauer für drei verschiedene Lastszenarien betrachtet. Beim ersten Szenario handelt es sich um ein Vollastszenario. Sobald Platz im Sendepuffer verfügbar ist, werden senderseitig von der Anwendung weitere Daten an die Transportschicht übergeben. Darüber hinaus erzeugt die Transportschicht einen gleichmäßigen Strom von Paketen. Dies wird erreicht, indem von der empfangenden Transportinstanz dem Sender neuer Sendekredit gewährt wird, sobald 2000 Bytes Pufferplatz im Empfangspuffer verfügbar sind.

Beim zweiten Szenario handelt es sich ebenfalls um ein Vollastszenario. Die Transportschicht erzeugt allerdings nicht wie im ersten Szenario einen gleichmäßigen Strom von Paketen, sondern sendet die Pakete burstartig. Die empfangende Transportinstanz gewährt erst dann dem Sender 24 KBytes neuen Kredit, sobald 24 KBytes im Empfangspuffer verfügbar sind. Als Folge ergibt sich ein Sendeburst von 24 KBytes und insgesamt ein burstartiger Strom von Paketen.

Das dritte Szenario ist ein Teillastszenario. Für jeden an die Transportschicht übergebenen Nutzdatenblock wird zufällig eine Übertragungsrate gewählt. Für die Bestimmung der Übertragungsrate wird eine normalverteilte Zufallsvariable mit dem Erwartungswert 2 Mbit/sec und der Standardabweichung 160 Kbit/sec herangezogen. Der nachfolgende Nutzdatenblock wird erst an die Transportschicht übergeben, nachdem die Zeitdauer vergangen ist, die unter Berücksichtigung der zufällig gewählten Rate für die Übertragung des vorangehenden Blocks erforderlich ist.

Abb. 5.17 zeigt gemittelt über 30 Meßläufe die Migrationsdauer in Abhängigkeit von der Übertragungsrate zwischen den beiden Transportgateways für die genannten drei Szenarien. Die Migration der Statusinformation erfolgt nebenläufig mittels der expliziten Migration. Für das gleichmäßige Vollastszenario ergibt sich eine längere Migrationsdauer als für das burstartige Vollastszenario. Im gleichmäßigen Vollastszenario sind bei jeder Migration die Puffer zum Migrationszeitpunkt nahezu komplett gefüllt. Darüber hinaus ändern sich die Pufferinhalte

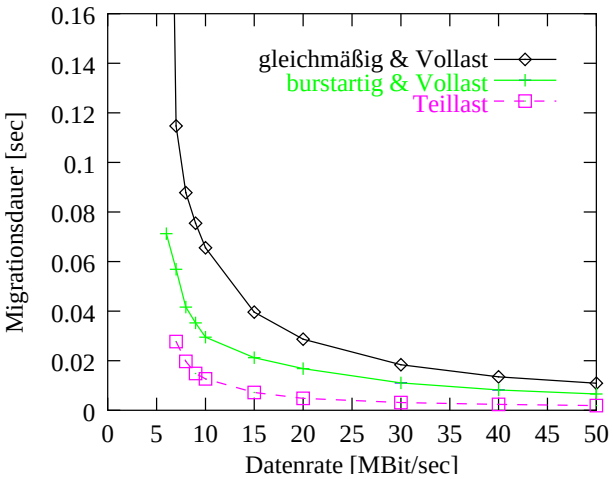


Abbildung 5.17: Auswirkungen verschiedener Lastprofile auf die Migrationsdauer

auf Grund der gleichmäßigen Transportkommunikation fortlaufend. Beim burstartigen Szenario sind die Puffer zum Migrationszeitpunkt nicht unbedingt komplett gefüllt und ändern sich nur, falls ein Burst von Paketen der Partnertransportinstanz eintrifft.

In Tabelle 5.5 ist für die drei Szenarien und verschiedene Übertragungsraten aufgeführt, wieviel Statusinformation im Mittel migriert wurde. Für die aufgeführten Übertragungsraten ist deutlich zu erkennen, daß im gleichmäßigen Vollastszenario mehr Statusinformation migriert werden muß als im burstartigen Vollastszenario und in diesem mehr als im Teillastszenario. In allen drei Szenarien reduziert sich die Menge der zu migrierenden Statusinformation mit zunehmender Übertragungsrate. Ursache hierfür ist die kürzere Migrationsdauer im Falle höherer Übertragungsraten. Die kürzere Migrationsdauer hat eine geringere Anzahl von Pufferänderungen zur Folge, die durch die nebenläufige Transportkommunikation bedingt sind. Auf Grund der geringeren Anzahl von Pufferänderungen ergibt sich eine geringere Menge zu migrierender Pufferinhalte.

Szenario	MBit/sec								
	6	7	8	9	10	20	30	40	50
gleichmäßig, Vollast	193.2	74.7	68.6	68.2	65.9	65.4	65.1	64.8	64.6
burstartig, Vollast	48.9	47.1	37.1	35.3	30.1	29.0	28.5	27.9	27.1
Teillast	17.7	17.7	15.1	13.3	13.3	12.9	12.1	11.2	11.2

Tabelle 5.5: Menge der migrierten Statusinformation

Auffallend hoch ist die Menge von 193.2 KBytes migrierter Statusinformation im gleichmäßigen Vollastszenario für eine Übertragungsrate von 6 Mbit/sec. Da es sich um ein Volllastszenario handelt und die Übertragungsrate von 2 Mbit/sec des Links zwischen der Basisstation und dem mobilen System den begrenzenden Faktor darstellt, erreichen die Nutzdaten das mobile System mit einer Rate von 2 Mbit/sec. Zwangsläufig ändern sich dann auch der Empfangspuffer bzw. der Sendepuffer der involvierten Transportinstanzen des Transportgateways mit einer Rate von 2 Mbit/sec. Die sich ändernden Puffer des alten Transportgateways müssen zum neuen Transportgateway migriert werden. Für die Migration der Puffer ist eine

Bandbreite von 2 * 2 Mbit/sec erforderlich. Zusammen mit den 2 Mbit/sec Bandbreite für die Transportkommunikation zwischen dem Transportgateway und dem mobilen System ist eine Bandbreite von 6 MBit/sec erforderlich. Da im diskutierten Szenario lediglich 6 Mit/sec zur Verfügung stehen, können die Puffer nicht wesentlich schneller migriert werden als sie sich ändern. Dies führt zu einer großen Menge zu migrierender Statusinformation und einer langen Migrationsdauer von im Mittel 0.37 sec. In Abb. 5.17 ist dieser Wert allerdings nicht mit aufgenommen, da andernfalls auf Grund der dann geänderten Skalierung die wesentlichen Details nur noch schwer zu erkennen wären. Steht die minimal erforderliche Bandbreite nicht zur Verfügung, so erkennt der Migrationsagent, daß die Migration nicht terminiert, und veranlaßt ein Verlangsamen der Transportkommunikation (siehe Kapitel 4.2.3.2).

Die Untersuchungen identifizieren das gleichmäßige Vollastszenario als das für die nebenläufige Migration schwerste Szenario der betrachteten drei Szenarien. Aus diesem Grunde liegt dieses Szenario sowohl den bereits beschriebenen Untersuchungen am Prototyp als auch den im nächsten Kapitel diskutierten Untersuchungen zur vergleichenden Bewertung der impliziten und der expliziten Migration zu Grunde.

5.3.5 Implizite vs. explizite Migration

Die in Kapitel 5.2.4 beschriebenen Untersuchungen am Prototyp ergaben hinsichtlich der Migrationsdauer und der Menge der migrierten Statusinformation keinen Vorteil der impliziten Migration gegenüber der expliziten Migration. Während bei den Untersuchungen am Prototyp die Migration unmittelbar nach dem Subnetzwechsel startet, wird bei den simulativen Untersuchungen die Migration erst zu einem späteren Zeitpunkt vorgenommen. Vom Zeitpunkt des Subnetzwechsels bis zum Migrationsstart wird im Falle der impliziten Migration das neue Transportgateway bereits über die Pufferinhalte informiert. Darüber hinaus bildet sich im simulativ untersuchten Szenario auf Grund der Bandbreitenunterschiede in der Basisstation eine Warteschlange. Eine Datenmenge im Umfang eines Flußkontrollfenster wird in der Warteschlange der Basisstation zwischengepuffert. Somit ergibt sich zwischen dem alten Transportgateway und dem mobilen System eine signifikant größere RTT als zwischen dem alten und dem neuen Transportgateway. Diese Unterschiede bzgl. der RTT waren beim mittels des Prototyps untersuchten Szenario nicht gegeben. Dies war mit eine Ursache dafür, daß dort die implizite der expliziten Migration nicht überlegen war.

Den simulativen Untersuchungen liegt ein gleichmäßiges Vollastszenario zu Grunde. Die maximale Größe der Puffer der zu migrierenden Transportinstanzen beträgt 32 KBytes. Die beobachteten Werte werden über 30 Simulationsläufe gemittelt. Das neue Transportgateway kann während dieses Zeitraumes von der impliziten Migration profitieren und die zwischen dem altem Transportgateway und dem mobilen System ausgetauschten Transportprotokollpakete mitlauschen.

In Tabelle 5.6 sind für die explizite und die implizite Migration die Migrationsdauer, die Menge der gesondert übertragenen Daten (Statusinformation) und die Unterbrechungsdauer dargestellt. Diese Werte sind für verschiedene Übertragungsraten zwischen dem alten und dem neuen Transportgateway aufgeführt. Hinsichtlich der Unterbrechungsdauer unterscheiden sich die implizite und die explizite Migration nicht wesentlich. Da die für die Unterbrechung verantwortliche Migration des Protokollkontrollblocks mit zunehmender Übertragungsrate schneller

	Migr.-variante	MBit/sec 6	7	8	9	10	20	30	40	50
Unterbrechung [ms]	explizit	6.3	6.2	6.1	6.1	6.1	6.0	6.0	6.0	6.0
	implizit	6.5	6.4	6.3	6.2	6.2	6.2	6.1	6.1	6.1
gesondert übertr. Daten [KBytes]	explizit	193.2	74.7	68.6	68.2	65.9	65.4	65.1	64.8	64.6
	implizit	100.7	61.3	56.0	51.9	49.3	46.5	44.9	45.1	44.1
Migrationsdauer [ms]	explizit	380	115	84	77	66	29	19	14	11
	implizit	208	94	72	57	48	21	13	10	9

Tabelle 5.6: Vergleich der expliziten und der impliziten Migration

erfolgen kann, ist für die Übertragungsrate von 50 Mbit/sec eine geringfügig geringere Unterbrechungsdauer als für die Rate 6 Mbit/sec zu beobachten.

Bei der expliziten Migration werden alle Pufferinhalte durch eine gesonderte Übertragung zum neuen Transportgateway migriert. Bei der impliziten Migration wird ein Teil der Statusinformation implizit migriert, ein weiterer Teil durch eine gesonderte Übertragung. Da für die gesonderte Übertragung – sowohl bei der impliziten als auch bei der expliziten Migration – zusätzlich Übertragungsressourcen notwendig sind, ist die Menge der gesondert übertragenen Statusinformation von Interesse. Die Werte in der Tabelle 5.6 verdeutlichen, daß im Fall der impliziten Migration weniger Daten gesondert übertragen werden müssen als bei der expliziten Migration. Dies ist die Ursache für die kürzere Migrationsdauer bei der impliziten Migration im Vergleich zur expliziten Migration. Obwohl die Statusinformation minimal 64 KBytes Puffer umfaßt, werden bei der impliziten Variante fast immer weniger als diese 64 KBytes durch gesonderte Übertragung migriert.

Ursache dafür, daß – abweichend von den Untersuchungen am Prototyp – die implizite Migration der expliziten Migration überlegen ist, sind die signifikant verschiedenen RTTs zwischen dem alten Transportgateway und dem mobilen System einerseits und dem alten Transportgateway und dem neuen Transportgateway andererseits. Aufgrund dieser Konstellation werden – abweichend vom dem am Prototyp untersuchten Szenario – implizit zum neuen Transportgateway migrierte Pufferinhalte nicht kurze Zeit später schon wieder aus dem Puffer der Transportinstanz beim alten Transportgateway gelöscht. Somit kann von der impliziten Migration der Pufferinhalte profitiert werden.

Die beschriebenen Simulationsergebnisse belegen, daß insbesondere im Fall geringer zur Verfügung stehender Bandbreiten zwischen dem alten und dem neuen Transportgateway die implizite Migration sinnvoll eingesetzt werden kann. Sowohl die Migrationsdauer als auch die Menge der gesondert übertragenen Statusinformation kann durch die implizite Migration reduziert werden.

5.4 Zusammenfassung

Die in diesem Kapitel beschriebenen Leistungsbewertungen können in zwei Kategorien eingeteilt werden. Zum einen in Messungen, die belegen, daß sich schnelle Subnetzwechsel realisieren lassen, die nur kurze Unterbrechungen der Netzwerkkonnektivität zur Folge haben. Zum

anderen in Untersuchungen, die zeigen, daß das OMIT-Konzept eingesetzt werden kann, um signifikante Unterbrechungen der Kommunikation in der Transportschicht auch im Fall der Mobilität der Endsysteme zu vermeiden.

Wird das Schnelle Agent Discovery Verfahren zusammen mit der Fast-Forwarding-Erweiterung von Mobile IP eingesetzt, kann die Unterbrechungsdauer der Netzwerkkonnektivität nach einem Subnetzwechsel signifikant reduziert werden. Indem im mobilen System eine schichtenübergreifende Signalisierung zwischen Mobile IP und dem Treiber, der die Netzwerkkarte für den Zugriff auf den Funkkanal steuert, realisiert wird, kann das Schnelle Agent Discovery Verfahren die Erkennung eines Subnetzwechsels seitens des mobilen Systems beschleunigen. Mittels des Fast-Forwarding-Verfahrens wird die Etablierung der Route in das neue Subnetz beschleunigt, da lediglich der geographisch nahe, alte Foreign Agent über die Einrichtung eines Forwarding-Tunnels informiert werden muß und nicht der unter Umständen weit entfernte Home Agent veranlaßt werden muß, die Pakete ins neue Subnetz zu tunneln. Beide Verfahren zusammen ermöglichen es, die durch Subnetzwechsel bedingte Unterbrechung der Netzwerkkonnektivität – unabhängig von der Entfernung zwischen Home Agent und mobilem System – auf ca. 25 ms zu reduzieren. Diese kürzeren Unterbrechungen sind nicht nur im Kontext des indirekten Transportansatzes von Nutzen, sondern auch für Ende-zu-Ende operierende Verbindungen. Der positive Einfluß auf UDP bzw. TCP wurde durch Messungen nachgewiesen.

Die Bewertung des OMIT-Konzeptes erfolgte sowohl anhand einer prototypischen Implementierung als auch mittels simulativer Untersuchungen. Da ein Teil der Untersuchungen sowohl am Prototyp als auch simulativ vorgenommen wurde und identische Ergebnisse geliefert hat, kann davon ausgegangen werden, daß weder implementierungsspezifische Details noch Unzulänglichkeiten der Modellierung die Ergebnisse verfälscht haben. Die Untersuchungen haben gezeigt, daß gleichmäßige Vollastszenarien – wie sie beispielsweise von einem FTP-Transfer verursacht werden – aufgrund der schnellen und andauernden Änderungen der Statusinformation in den Transportinstanzen des Transportgateways besonders problematisch für die nebenläufige Migration sind. Aus diesem Grunde konzentrierten sich die Untersuchungen im wesentlichen auf das gleichmäßige Vollastszenario. Sowohl die Vermessung des Prototyps als auch die Simulationsergebnisse ergaben, daß sich mittels der nebenläufigen Migration – unabhängig von der maximalen Puffergröße – konstante Unterbrechungszeiten in der Größenordnung von ca. 10 ms erzielen lassen. Dies gilt sowohl für die implizite als auch für die explizite Migration. Wie erwartet verlängert sich die Migrationsdauer bei der nebenläufigen Migration im Vergleich zur Migration mit Einfrieren. Weiterhin zeigen die Untersuchungen, daß die implizite Migration nur unter bestimmten Randbedingungen der expliziten Migration überlegen ist. Die implizite Migrationsstrategie ist dann sinnvoll einsetzbar, falls die RTT zwischen dem alten Transportgateway und neuen Transportgateway signifikant geringer ist als die RTT zwischen altem Transportgateway und dem mobilen System.

Kapitel 6

Zusammenfassung und Ausblick

6.1 Zusammenfassung und Ergebnisse

Die vorliegende Arbeit behandelt die Thematik der drahtlosen Anbindung mobiler Systeme an das Internet. Der Fokus der Betrachtungen liegt auf der zuverlässigen Datenkommunikation. Da – im Vergleich zur drahtgebundenen Kommunikation – die drahtlose Kommunikation fehleranfälliger ist, stellt sich die Frage, inwieweit das Transportprotokoll TCP, das Ende-zu-Ende einen zuverlässigen Dienst zur Verfügung stellt, mit dieser höheren Fehleranfälligkeit zurechtkommt. Ursache für die höhere Fehleranfälligkeit sind schwankende und höhere Bitfehlerraten auf dem Funkkanal und temporäre Unterbrechungen, die z.B. durch Funkschatten, temporäres Verlassen des Funkabdeckungsbereiches oder fehlendes Forwarding in Multi-Hop-Netzwerken bedingt sein können. Im Kontext dieser höheren Fehleranfälligkeit erweist sich TCP als problematisch, da es nach durch Bitfehler bedingten Paketverlusten eine Lastreduktion mittels der Mechanismen Slow Start und Congestion Avoidance vornimmt. Darüber hinaus nimmt TCP nach längeren Unterbrechungen nicht unmittelbar am Ende der Unterbrechung des Übertragungskanals, sondern erst zu einem späteren Zeitpunkt die Kommunikation wieder auf und reduziert zusätzlich den Slow-Start-Grenzwert auf seinen Minimalwert. Aus diesem Grund entfällt die Phase der exponentiellen Öffnung des Lastkontrollfensters. Stattdessen steuert die Congestion Avoidance von TCP die Öffnung des Lastkontrollfensters. Dies hat eine langsame, lineare Öffnung des Fensters und unnötige Durchsatzeinbußen zur Folge.

Eine Vielzahl von Lösungsansätzen ist in der Literatur für die skizzierten Probleme beschrieben. Diese Ansätze erfordern allerdings zum Teil erhebliche Änderungen – über die mobilen Systeme hinausgehend – an Routern innerhalb des Internets bzw. an Festnetzrechnern, die potentielle Kommunikationspartner der mobilen Systeme sind. Auf Grund der erforderlichen Änderungen an im Internet installierten Systemen ist der Einsatz dieser Verfahren nur schwer und in einem langwierigen Prozeß durchzusetzen.

In der vorliegenden Arbeit liegt der Fokus auf Ansätzen, die *ohne* Änderungen an allen potentiellen Kommunikationspartnern der mobilen Systeme die oben skizzierten Probleme von TCP im Kontext der drahtlosen Kommunikation zu lösen versuchen. In einem ersten Schritt wurden in der vorliegenden Arbeit die verschiedenen, in der Literatur beschriebenen Lösungsansätze klassifiziert und dahingehend bewertet, inwieweit sie auf massive Änderungen an im Internet installierten Systemen verzichten können. Der indirekte Transportansatz kristallisierte sich bei diesen Betrachtungen als der Ansatz der Wahl heraus.

Der indirekte Transportansatz erlaubt es, ohne die Interoperabilität zu TCP-basierten Systemen im Internet zu verlieren, ein spezielles Transportprotokoll zu verwenden, das über der drahtlosen Übertragungsstrecke operiert und sowohl Unterbrechungen als auch die höheren Bitfehlerraten angemessen berücksichtigt. Da bereits einige Arbeiten sich mit derartigen speziellen Transportprotokollen befaßt haben, war es nicht das Ziel der vorliegenden Arbeit, ein weiteres hierfür geeignetes Transportprotokoll zu entwickeln.

Fokus der eigenen Arbeiten war es, ein Rahmenwerk zu schaffen, das eine Mobilitätsunterstützung für indirekte Transportansätze bietet. Im Kontext der Mobilität der Endsysteme ist die in den beiden Transportinstanzen eines Transportgateways für eine indirekte Transportverbindung verwaltete Statusinformation problematisch. Ändert sich auf Grund der Mobilität eines Endsystems das Routing, müssen entsprechende Maßnahmen ergriffen werden, damit trotzdem die Statusinformation auf dem als Transportgateway fungierenden System verfügbar ist. Bei existierenden indirekten Ansätzen ist die Mobilität der Endsysteme nicht angemessen berücksichtigt. Dies äußert sich in Unterbrechungen von bis zu 1400 ms, die durch die Mobilität der Endsysteme bedingt sind. Hier setzt das in der vorliegenden Arbeit entwickelte OMIT-Konzept (**O**ptimierte **M**obilitätsunterstützung für **I**ndirekte **T**ransportansätze) mit dem Ziel der Reduktion dieser Unterbrechungszeiten an. OMIT verwendet zwei Strategien, um die durch die Mobilität der Endsysteme bedingten Unterbrechungen in der Transportkommunikation zu reduzieren: Das sogenannte *Fast Forwarding* und die *nebenläufige Migration*.

Mittels des *Fast Forwardings* wird in das Routing eingegriffen, so daß auch nach Subnetzwechseln das Transportgateway, das vor dem Subnetzwechsel als Transportgateway fungiert hat, weiterhin als Transportgateway operieren kann. Wechselt ein mobiles System in ein neues Subnetz, wird ein sogenannter *Forwarding Tunnel* zwischen dem alten und dem neuen Subnetz etabliert. Trotz des Subnetzwechsels werden an das mobile System adressierte Pakete weiterhin in das alte Subnetz gesendet und von dort in das neue Subnetz weitergeleitet. Das im alten Subnetz lokalisierte Transportgateway liegt weiterhin im Datenpfad und kann damit noch als Transportgateway fungieren. Die durch die Mobilität der Endsysteme bedingte Unterbrechung beschränkt sich auf die Zeitdauer, die zur Etablierung des Forwarding-Tunnels erforderlich ist. Das Fast-Forwarding-Konzept wurde in Mobile IP integriert. Es wird der Foreign-Agent-Modus von Mobile IP vorausgesetzt. Um zwischen dem alten und dem neuen Foreign Agent den Forwarding Tunnel einzurichten, verständigen sich die beiden Foreign Agents durch das neu definierte *Fast-Forwarding-Protokoll*. Im Falle wiederholter Subnetzwechsel können sich Forwarding-Ketten und auch Schleifen in diesen Ketten ergeben. Wie diese Ketten bzw. Schleifen zu behandeln sind und wie sie aufgelöst werden können, wurde in der vorliegenden Arbeit ebenfalls betrachtet. Die Fast-Forwarding-Erweiterung von Mobile IP bietet eine schnellere Wiederherstellung – innerhalb von weniger als 10 ms – der Netzwerkkonnektivität als Mobile IP ohne diese Erweiterung und ermöglicht es darüber hinaus, trotz Subnetzwechseln das alte Transportgateway weiter nutzen zu können. Eine Migration zu einem späteren Zeitpunkt ist dennoch möglich. Der Zeitpunkt des Subnetzwechsel ist aber vom Zeitpunkt der Migration entkoppelt.

Die *nebenläufige Migration* ermöglicht mit konstanten Unterbrechungszeiten von ca. 10 ms, d.h. ohne die genannten inakzeptablen Unterbrechungen von 1400 ms in Kauf nehmen zu müssen, die Transportinstanzen einer indirekten Transportverbindung von einem Transportgateway auf ein anderes Transportgateway zu verlagern, so daß das neue Transportgateway die Kopplung der Transportinstanzen übernehmen kann. Das ist inbesondere dann sinnvoll, falls sich eine lange Forwarding-Kette gebildet hat und das Transportgateway auf einen näher beim

mobilen System lokalisierten Foreign Agent verlagert werden soll. Grundidee der nebenläufigen Migration ist es, die Migration zeitlich parallel zur weiterhin aktiven Transportkommunikation vorzunehmen. Problematisch ist in diesem Kontext, daß sich die zu migrierenden Pufferinhalte auf Grund der weiterhin aktiven Transportkommunikation während der Migration verändern. Spezielle Mechanismen sind realisiert, um trotzdem sicherzustellen, daß beim neuen Transportgateway ein identisches Abbild der Statusinformation verfügbar gemacht werden kann und das neue Transportgateway die Kopplung der Transportinstanzen übernehmen kann. Sowohl bei der *expliziten Migration* als auch bei der *impliziten Migration* erfolgt die Migration der Statusinformation nebenläufig. Diese beiden Varianten unterscheiden sich hinsichtlich der Menge an Statusinformation, die zum neuen Transportgateway übertragen werden muß.

Die Architektur eines *OMIT-Transportgateways*, in dem Mobile IP zusammen mit dem Fast-Forwarding-Konzept und dem Konzept der nebenläufigen Migration eine optimierte Mobilitätsunterstützung für indirekte Transportansätze bietet, wurde darüber hinaus in der vorliegenden Arbeit entwickelt. Insbesondere die Interaktion der genannten Komponenten ist in diesem Kontext von Bedeutung, da diese Komponenten in den verschiedenen Phasen der Migration jeweils verschiedene Aufgaben zu übernehmen haben. Im sogenannten *Migrationsagenten* ist die explizite bzw. die implizite Migrationsstrategie realisiert. Weiterhin übernimmt er die Übertragung der Statusinformation zum neuen Transportgateway, aktiviert bzw. deaktiviert die Transportinstanzen und steuert, wann Pakete eines mobilen Systems lokal in den Transportinstanzen des Transportgateways bearbeitet werden bzw. mittels Fast Forwarding zu einem anderen Foreign Agent gesendet werden und dort an die Transportinstanzen übergeben werden.

Die Leistungsbewertung anhand der Vermessung der prototypischen Implementierung bzw. der simulativen Untersuchungen hat gezeigt, daß das OMIT-Konzept die Erwartungen erfüllen kann. Mittels der nebenläufigen Migration lassen sich konstante Unterbrechungszeiten in der Größenordnung von ca. 10 ms unabhängig von der Größe und dem Füllungsgrad der Sende- bzw. Empfangspuffer der zu migrierenden Transportinstanzen erreichen. Durch das Fast Forwarding können Migrationen vermieden werden. Darüber hinaus kann mittels der Fast-Forwarding-Erweiterung von Mobile IP die Konnektivität in der Netzwerkschicht schneller wiederhergestellt werden als ohne diese Erweiterung. Hiervon profitiert nicht nur der indirekte Transportansatz, sondern auch die Ende-zu-Ende operierenden Protokolle UDP und TCP.

Zusammenfassend kann festgehalten werden, daß die vorliegende Arbeit ein Rahmenwerk bietet, um den indirekten Transportansatz auch für mobile Systeme einzusetzen. Die Verfahren sind nicht auf einen speziellen indirekten Transportansatz zugeschnitten, sondern für indirekte Transportansätze im allgemeinen verwendbar. Mittels des OMIT-Konzeptes können trotz der beim indirekten Transportansatz im Transportgateway zu verwaltenden Statuinformationen Subnetzwechsel mobiler Systeme ohne signifikante Unterbrechungen realisiert werden. Das Konzept ist allerdings relativ aufwendig zu realisieren.

6.2 Ausblick

Mögliche Erweiterungen und offene Fragestellungen im Kontext des OMIT-Konzeptes werden in diesem Abschnitt zum Abschluß kurz skizziert. Gegenstand weiterer Untersuchungen kann die Bestimmung eines geeigneten Migrationszeitpunktes sein. Darüber hinaus ist die Frage der Vereinbarkeit der Konzepte von OMIT, die auf die Mobilitätsunterstützung auf Basis von Mobile IP zugeschnitten sind, mit einer Mobilitätsunterstützung zu klären, die auf Hierarchien von Foreign Agents [AFH+99] oder auf IPv6 [JP00] basiert.

Der Migrationszeitpunkt kann in OMIT auf Grund des Fast-Forwarding-Konzeptes frei gewählt werden. Ursache ist die Entkopplung des Zeitpunktes der Migration von dem Zeitpunkt, zu dem ein Subnetzwechsel des mobilen Systems stattfindet. Diese Freiheit läßt allerdings die Frage aufkommen, welcher Zeitpunkt für eine Migration günstig ist und welche Kriterien für die Entscheidung heranzuziehen sind, wann eine Migration vorzunehmen ist. Die RTT zwischen dem Transportgateway und dem mobilen System könnte ein mögliches Kriterium für eine Migration sein. Zu berücksichtigen wären hierbei die Anforderungen des zwischen dem Transportgateway und dem mobilen System operierenden Transportprotokolls. Darüber hinaus könnte die Auslastung des aktuell als Transportgateway fungierenden Systems in die Entscheidung mit einfließen, ob eine Migration zu einem anderen Transportgateway sinnvoll ist. Sofern Informationen über das Bewegungspattern des mobilen Systems verfügbar sind, ist eventuell sinnvoll, diese bei der Entscheidung bzgl. einer Migration ebenfalls mit zu berücksichtigen.

Inwieweit hierarchische Konzepte für die Mobilitätsunterstützung [AFH+99] sich zusammen mit dem OMIT-Konzept vereinen lassen, ist eine weitere interessante Fragestellung. Zu klären ist hier primär die Frage, inwieweit sichergestellt werden kann, daß trotz eines Subnetzwechsels das alte Transportgateway weiterhin im Datenpfad liegt. Ist dies gewährleistet, so kann das Konzept der nebenläufigen Migration weiterhin angewandt werden. Bei hierarchischen Konzepten bietet sich die Möglichkeit, die Hierarchieebene des Foreign Agents, auf dem ein Transportgateway für ein mobiles System realisiert wird, gezielt in Abhängigkeit von dem Grad der Mobilität eines Endsystems zu wählen. Hochgradig mobile Endsysteme verwenden einen Foreign Agent auf einer höheren Ebene als Transportgateway in der Hoffnung, daß trotz eines Subnetzwechsels die Pakete über diesen Foreign Agent geroutet werden und somit keine Migration erforderlich wird. Weniger mobile Systeme wählen wegen der besseren Skalierung einen Foreign Agent auf einer niedrigeren Hierarchieebene als Transportgateway. Die Zuordnung eines Endsystems zur Gruppe der mobilen bzw. weniger mobilen Systeme kann ggf. dynamisch vorgenommen werden.

Die Mobilitätsunterstützung von IPv6 [JP00] läßt sich nicht ohne Probleme zusammen mit dem OMIT-Konzept einsetzen. Ursache hierfür ist die Tatsache, daß in IPv6 kein ausgewiesenes System – wie der Foreign Agent in Mobile IP für IPv4 – existiert, über das Pakete des mobilen Systems garantiert geroutet werden. Somit ist unklar, auf welchem System das Transportgateway realisiert werden kann. Kommt hingegen eine hierarchische Variante der Mobilitätsunterstützung von IPv6 [SC+00] zum Einsatz, kann auf dem sogenannten Mobility Anchor Point, über den alle Pakete des mobilen Systems geroutet werden, das Transportgateway realisiert werden. Inwieweit sich dann die Verfahren des OMIT-Konzeptes anwenden lassen, bedarf allerdings weiterer Untersuchungen.

Anhang A

Mobile IP mit Fast Forwarding

A.1 Protokolldateneinheiten

In diesem Teil des Anhangs wird auf die von Mobile IP verwendeten Protokolldateneinheiten eingegangen. Es werden sowohl die wesentlichen Protokolldateneinheiten von Mobile IP als auch die für die Realisierung des Fast-Forwarding-Konzeptes zusätzlich erforderlichen Protokolldateneinheiten beschrieben.

A.1.1 Mobile IP Protokolldateneinheiten

A.1.1.1 Agent Advertisement Erweiterung

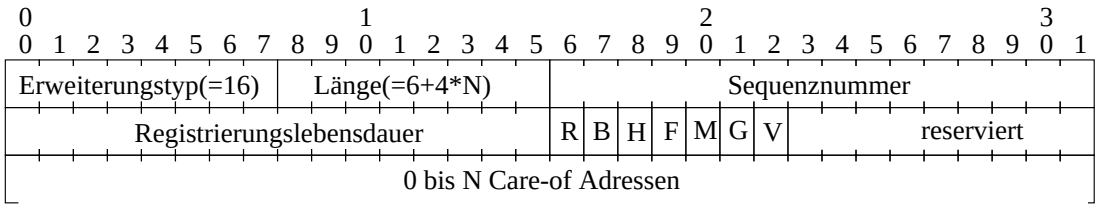


Abbildung A.1: Format einer Agent Advertisement Erweiterung

Abb. A.1 zeigt das Datenformat der Agent Advertisement Erweiterung. Im Typfeld wird der Erweiterungstyp kodiert, mittels des Längenfeldes kann die Startposition der ggf. folgenden Erweiterung bestimmt werden. Im Sequenznummernfeld wird die Anzahl der seit dem Start des Agents ausgesandten Advertisements hochgezählt. Der Verlust einzelner Advertisements kann anhand des Sequenznummernfeldes auf dem mobilen System erkannt werden, sobald ein nachfolgendes Advertisement empfangen wird. Die in Sekunden angegebene Lebensdauer eines Advertisements wird in dem Feld *Registrierungslebensdauer* abgelegt. Diese Lebensdauer dient dem mobilen System als Anhaltspunkt, wann die nächsten periodisch ausgesandten Advertisements eintreffen müßten. Treffen sie nicht ein, ist dies ein Hinweis auf einen Subnetzwechsel. Wird der Foreign-Agent-Modus unterstützt, so wird die Care-of-Adresse ebenfalls in der Nachricht kodiert. Mittels des Bitfeldes wird das mobile System informiert, welche Optionen der Mobility Agent unterstützt:

- R-Bit
  Der Colocated-Modus ist in diesem Subnetz nicht nutzbar. Ein mobiles System muß seine Care-of-Adresse vom Foreign Agent erhalten.

- B-Bit
  Der Mobility Agent ist überlastet und kann das mobile System nicht unterstützen.

- H-Bit bzw. F-Bit
  Der Agent fungiert in dem Subnetz, in das die Advertisements gesendet werden, als Home Agent bzw. als Foreign Agent.

- M-Bit bzw. G-Bit
  Für das Mobile IP Routing ist ein Tunnelmechanismus notwendig. Hierfür stehen prinzipiell verschiedene Varianten zur Verfügung. Das M-Bit bzw. G-Bit kodiert, welche dieser Varianten vom Agenten unterstützt werden.

- V-Bit
  Mittels diese Bits erfährt das mobile System, ob der Agent die Van Jacobson Header Komprimierung [Jac90] unterstützt.

A.1.1.2 Registrierungsanforderung

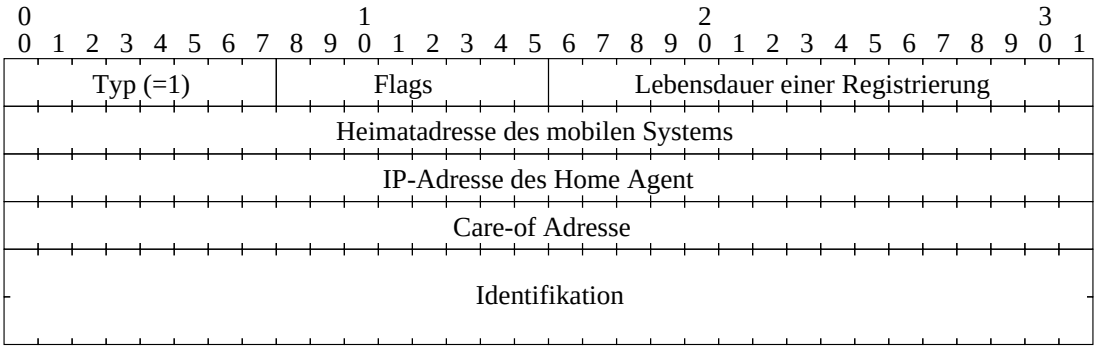


Abbildung A.2: Format einer Registrierungsanforderung

Abb. A.2 zeigt den Aufbau einer Registrierungsanforderung. Das Typfeld dient der Unterscheidung der verschiedenen Mobile IP-Nachrichten. Registrierungsanforderungen tragen den Wert 1 im Typfeld. Mittels der Flags können verschiedene Optionen vom mobilen System angefordert werden.

- S-Bit
  Ist dieses Bit gesetzt, so werden alte bestehende Registrierungen beim Home Agent nicht gelöscht. Stattdessen wird die neue Registrierung der Liste der bestehenden Registrierungen hinzugefügt.

- B-Bit
  Sollen neben den an das System adressierten Paketen auch im Heimatsubnetz ausgesendete Broadcasts an den aktuellen Aufenthaltsort weitergeleitet werden, so kann dies durch Setzen des B-Bits angefordert werden.

- D-Bit
  Unterstützt ein mobiles System die Entkapselung von Daten und soll der Colocated-Modus von Mobile IP für die Mobilitätsunterstützung dieses mobilen Systems zum Einsatz kommen, so wird dies durch Setzen des D-Bits zum Ausdruck gebracht.

Das M-Bit, das G-Bit und das V-Bit haben eine identische Bedeutung wie bei den in Abb. A.1 dargestellten Mobile IP-Advertisements. In dem Feld Lebensdauer wird kodiert, wie lange die Registrierung beim Agenten gültig sein soll, d.h. wie lange keine Erneuerung der Registrierung durch eine erneute Registrierungsanforderung erforderlich ist. Die Heimatadresse muß in der Registrierungsnachricht kodiert sein, da anhand dieser Adresse die Agenten bestimmen, für welches mobile System die Mobilitätsunterstützung angefordert wird. Die IP-Adresse des Home Agents muß in der Nachricht kodiert sein, damit im Falle des Foreign-Agent-Modus der Foreign Agent ermitteln kann, an welchen Home Agent eine vom mobilen System empfangene Registrierungsnachricht gesendet werden muß. Mittels der Care-of-Adresse wird der Home Agent darüber informiert, an welches System er für ein mobiles System bestimmte Pakete tunneln muß. In Abhängigkeit vom D-Bit dieser Registrierungsnachricht handelt es sich hierbei entweder um eine Foreign-Agent-Care-of-Adresse oder um eine Colocated-Care-of-Adresse. Um Sicherheitsmechanismen zu realisieren wird das Identifikationsfeld genutzt.

A.1.1.3 Registrierungsantwort

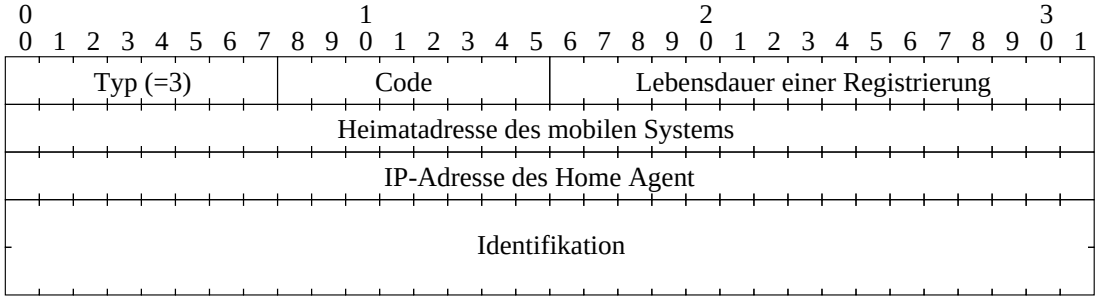


Abbildung A.3: Format einer Registrierungsantwort

In Abb. A.3 ist eine Registrierungsantwort dargestellt. Der Wert 3 im Typfeld kennzeichnet diese Mobile IP-Nachricht als Registrierungsantwort. Der Wert des Codefeldes beschreibt, ob ein Home Agent bzw. Foreign Agent die in der Registrierungsanforderung angeforderte Mobilitätsunterstützung mit den jeweiligen Optionen unterstützten kann oder ablehnt. Der Wert 0 kennzeichnet die Akzeptanz der jeweiligen Registrierung, ein von 0 verschiedener Wert kodiert die Ablehnung und den jeweiligen Ablehnungsgrund. Die Felder Heimatadresse, IP-Adresse des Home Agents und das Identifikationsfeld haben die gleiche Bedeutung wie in der Registrierungsanforderung.

A.1.2 Protokolldateneinheiten für das Fast Forwarding

Die im folgenden aufgeführten Formate sind zusätzlich zu den in Mobile IP definierten eingeführt worden. Sie sind erforderlich, um das Fast-Forwarding-Protokoll bzw. die Schleifenauflösung zu realisieren.

A.1.2.1 Alte Foreign Agent Erweiterung

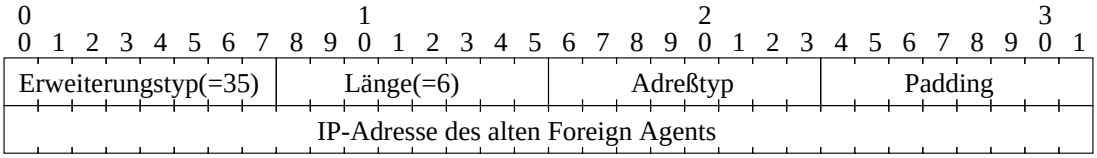


Abbildung A.4: Alte Foreign Agent Erweiterung

Abb. A.4 zeigt die Erweiterung, die vom mobilen System an die Registrierungsanforderung angehängt wird, damit der neue Foreign Agent über die Adresse des alten Foreign Agent Kenntnis erlangt und anschließend der neue Foreign Agent die Einrichtung eines Fast-Forwarding-Tunnels veranlassen kann. Die ersten 8 Bit legen den Typ der Erweiterung fest, die folgenden 8 Bit die Länge der Erweiterung. Zweck des Padding Feldes ist es, die nachfolgend kodierte IP-Adresse auf einer 32 Bit Grenze beginnen zu lassen. Welche IP-Adresse in der Erweiterung kodiert ist, spiegelt das Feld Adreßtyp wieder. Mögliche Werte sind:

- ISINVALID
  Vor dem Subnetzwechsel ist das mobile System bei keinem Foreign Agent angemeldet gewesen. Aus diesem Grunde wird keine IP-Adresse im Adreßfeld kodiert.
- ISREREGISTER
  Bei der Registrierung handelt es sich um eine Wiederholung der Registrierung des mobilen Systems bei einem Foreign Agent, bei dem das mobile System zuvor schon angemeldet war. Da kein Subnetzwechsel stattgefunden hat braucht kein Forwarding Tunnel etabliert werden und keine IP-Adresse dem Foreign Agent bekannt gemacht werden.
- ISOLDFA
  Das mobile System ist in ein neues Subnetz gewechselt. Die im Adreßfeld kodierte IP-Adresse ist die IP-Adresse des alten Foreign Agent. Der neue Foreign Agent benötigt diese, um den Aufbau eines Forwarding Tunnels zwischen dem alten und dem neuen Foreign Agent zu veranlassen.

A.1.2.2 Fast Forwarding Notify Protokolldateneinheiten

Bei der in Abb. A.5 dargestellten Nachricht handelt es sich nicht um eine Erweiterung, die an eine Mobile IP Nachricht angehängt wird, sondern um eine eigenständige Protokolldateneinheit. Sie wird als UDP-Paket zwischen dem alten Foreign Agent und dem neuen Foreign Agent ausgetauscht.

Für das Fast-Forwarding-Protokoll sind die folgenden drei Notifytypen erforderlich:

- Fast Forwarding Notify
  Diese Nachricht hat den Notifytyp 2 und wird vom alten zum neuen Foreign Agent übertragen, um das Fast Forwarding anzufordern.
- Fast Forwarding Acknowledge
  Kann der alte Foreign Agent das Fast Forwarding unterstützen, sendet er diese Nachricht (Notifytyp 3) an den neuen Foreign Agent.

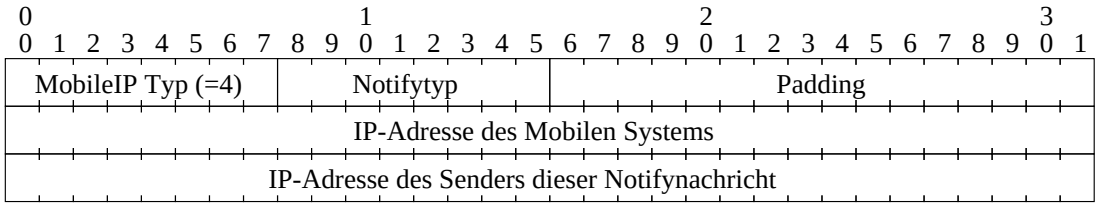


Abbildung A.5: Fast Forwarding Notify Protokolldateneinheiten

- Fast Forward Negative Acknowledge
  Im Fall einer Ablehnung des Fast Forwardings sendet der alte Foreign Agent diese negative Bestätigung (Notifytyp 4) zum neuen Foreign Agent.

A.1.2.3 Schleifenerkennung Erweiterung

Abb. A.6 zeigt die Erweiterung, die für die Schleifenerkennung verwendet wird. Jeder Foreign Agent, den eine Registrierungsantwort passiert, hängt eine solche Erweiterung zusätzlich an die Registrierungsantwort an.

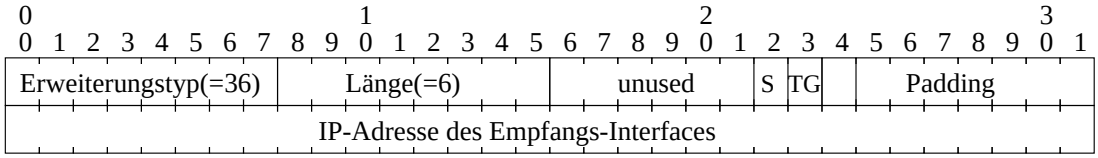


Abbildung A.6: Schleifenerkennung Erweiterung

Als IP-Adresse wird die IP-Adresse des Interfaces eingetragen, über das die Registrierungsnachricht empfangen wurde. Zusätzlich werden ggf. die beiden Status-Bits gesetzt.

- S-Bit
  Dieses Bit wird von vom Foreign Agent in der Erweiterung gesetzt, falls der Foreign Agent durch Auswerten der bereits an der Registrierungsantwort angehängten Schleifenerkennung-Erweiterung erkennt, daß die Registrierungsantwort bereits zum zweiten mal den Foreign Agent passiert und somit eine Schleife vorliegt.

- TG-Bit
  Dieses Bit wird vom Foreign Agent in der Erweiterung gesetzt, falls der Foreign Agent für Transportverbindungen des mobilen Systems als Transportgateway fungiert.

Anhang B

Visualisierungstool für Sim PlusPlus

Das Visualisierungstool für die Simulationsumgebung Sim PlusPlus [Ros92a] mit der Erweiterung SimEnv [Ros92b] wurde entwickelt, um Simulationsabläufe besser verfolgen zu können und das Debugging zu erleichtern. Die in der Beschreibungssprache von SimEnv definierte Netztopologie, d.h. die Netzwerkknoten und die Leitungen zwischen diesen Knoten können graphisch dargestellt werden. Darüber visualisiert das Werkzeug welche Protokollschichten innerhalb eines Knotens realisiert sind und zwischen welchen Protokollschichten Protokolldateneinheiten ausgetauscht werden. In einem Einzelschrittmodus kann der Ablauf einer Simulation gesteuert werden. Abb. B.1 zeigt das Hauptfenster des Visualisierungstools mit einer simulativ untersuchten Netztopologie.

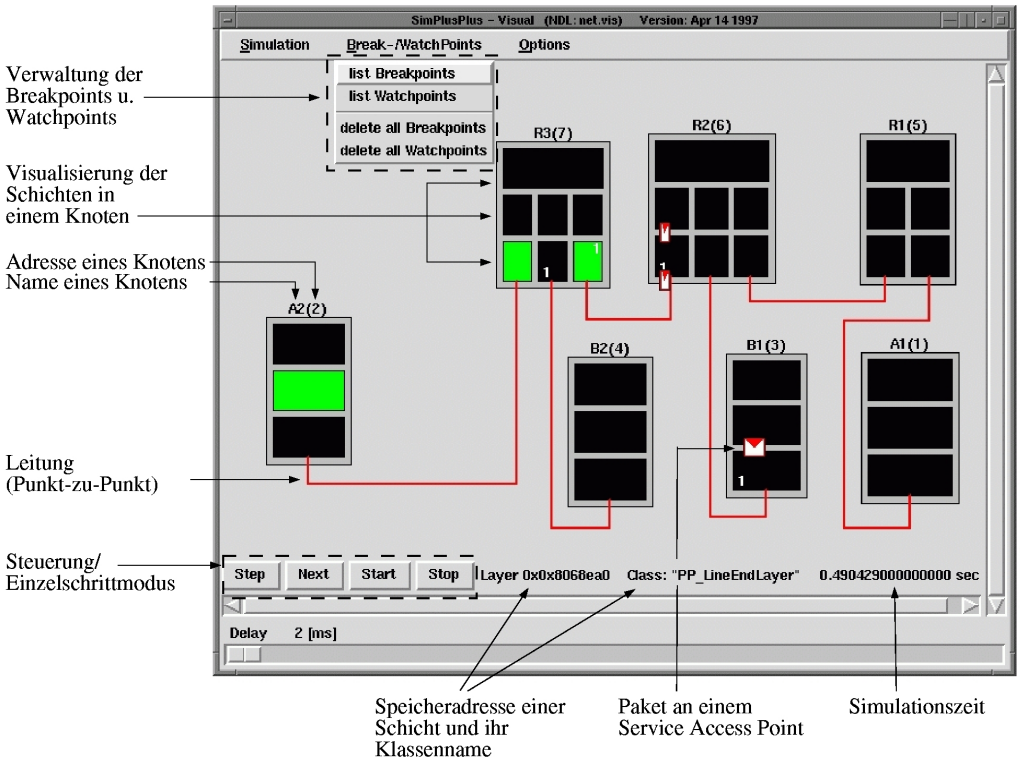


Abbildung B.1: Visualisierung mit Sim PlusPlus (Hauptfenster)

Das Visualisierungstool beschränkt sich darauf, Vorgänge zwischen den Protokollschichten, d.h. die Übergabe von Paketen zwischen den Protokollschichten und zwischen verschiedenen Knoten zu visualisieren. Schichteninterne Vorgänge, die mittels der Konstrukte von Sim PlusPlus modelliert werden, können von dem Werkzeug nicht dargestellt werden. Diese Einschränkung ist dadurch bedingt, daß bei der Entwicklung des Werkzeuges es als eine wesentliche Anforderung angesehen wurde, das in C++ realisierte Simulationsmodell nicht massiv um für die Visualisierung erforderlichen Code erweitern zu müssen. Der Austausch von Protokolldateneinheiten zwischen den benachbarten Schichten wird automatisch – ohne daß die explizite vom Programmierer kodiert werden muß – an das in Tcl/Tk realisierte Visualisierungstool gemeldet und graphisch dargestellt. Für eine Visualisierung schichteninterner Vorgänge hätte das für die Visualisierung erforderliche Detailwissen nicht vor dem Programmierer verborgen werden können. Aus diesem Grunde wurde auf die Visualisierung schichteninterner Vorgänge verzichtet.

Das Tool erlaubt es, die Simulation im Einzelschrittmodus zu steuern oder bis zu einer bestimmten Simulationszeit ohne Unterbrechung laufen zu lassen. Im Einzelschrittmodus stoppt die Simulation, sobald eine Protokolldateneinheiten zwischen zwei benachbarten Protokollschichten bzw. zwischen zwei Knoten ausgetauscht wird. Darüber hinaus können zwei verschiedene Typen von Breakpoints gesetzt werden. Zum einen Breakpoints auf Pakete, zum anderen Breakpoints auf die Schnittstelle zwischen benachbarten Schichten. Im Falle eines Breakpoints auf ein Paket stoppt die Simulation, sobald dieses Paket zwischen zwei benachbarten Protokollschichten ausgetauscht wird. Im Falle eines Breakpoints zwischen zwei benachbarten Schichten stoppt die Simulation, sobald ein beliebiges Paket zwischen diesen beiden Schichten ausgetauscht wird. Abb. B.2 zeigt beide Arten von Breakpoints, die anhand der Speicheradresse des Pakets bzw. der Speicheradressen der benachbarten Protokollschichten identifiziert werden.

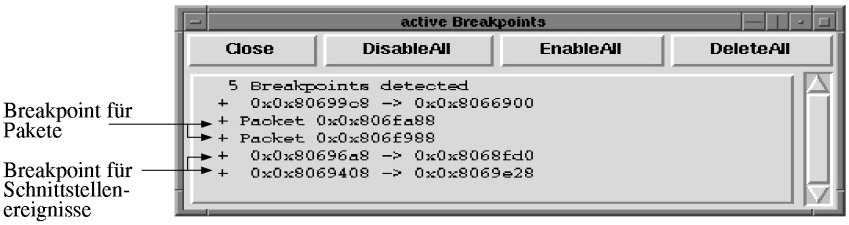


Abbildung B.2: Breakpoints

Zusätzlich zur Steuerung der Simulation bietet das Tool die Möglichkeit, Detailinformation (Variablenwerte) bzgl. der ausgetauschten Pakete bzw. der Schichten eines Knotens anzufordern. Damit das Visualisierungstool diese Detailinformation bei Sim PlusPlus anfordern kann, müssen die zugehörigen Variablenwerte registriert werden. Dies muß der Programmierer – allerdings nur einmalig im Konstruktor des Paketes bzw. der Protokollschicht – entsprechend kodieren. Abb. B.3 zeigt exemplarisch Detailinformation zur Sim PlusPlus-Klasse *PP_LineEndLayer*. Im Konstruktor dieser Klasse wurden von Programmierer die Variablen *delay* und *rate* registriert. Vom Visualisierungstool aus können die Detailinformation dieser Protokollschicht abgefragt werden und somit die aktuellen Werte der Variablen ermittelt werden. Analog kann auch vorgegangen werden, um die in einem Paket kodierten Variablenwerte zu ermitteln. Bei Paketen können auch für Pakete höherer Protokollschichten, die eingekapselt sind, die aktuellen Variablenwerte bestimmt werden.

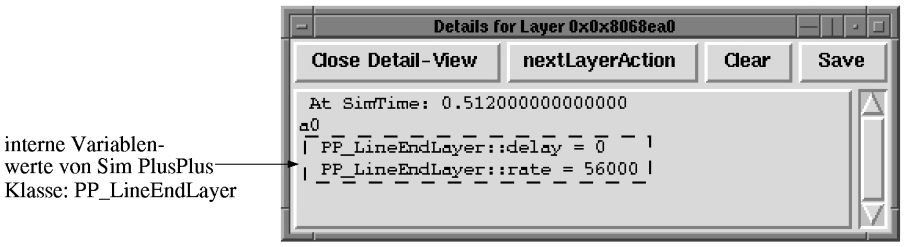


Abbildung B.3: Detailinformation im Visualisierungstool

Das Visualisierungstool eignet sich insbesondere dazu zu verfolgen, welche einzelnen Protokollschichten der verschiedenen Knoten einzelne Pakete passieren. Die Möglichkeit, Breakpoints auf einzelne Pakete zu setzen, erweist sich hierbei als sinnvoll. Um die innerhalb einer Schicht modellierten Vorgänge nachvollziehen zu können, ist es allerdings zusätzlich notwendig, den Simulationsablauf im Debugger bzw. anhand von Debugausgaben zu verfolgen. Das Visualisierungstool kann zusammen mit dem Debugger eingesetzt werden. Im Einzelschrittmodus und mit Hilfe von Breakpoints kann relativ einfach zu der Phase der Simulation, die im Detail untersucht werden soll, navigiert werden, um anschließend die schichteninternen Vorgänge im Debugger zu verfolgen. Der gemeinsame Einsatz des Visualisierungstools zusammen mit den Debugger erweist sich hier als sinnvoll.

Abkürzungsverzeichnis

ACK	Acknowledgement
AFE	Alte Foreign Agent Erweiterung (Mobile IP)
AMPS	Advance Mobile Phone System
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BS	Basisstation
CDMA	Code Division Multiple Access
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CWND	Congestion Window (TCP)
DAB	Digital Audio Broadcast
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DoS	Denial-of-Service
DVB	Digigal Video Broadcast
ECN	Explicit Congestion Notification
EDGE	Enhanced Data rates for GSM Evolution
ELN	Explicit Loss Notification
ETSI	European Telecommunications Standards Institute
F-TPI	F-Transportinstanz
FA	Foreign Agent
FEC	Forward Error Correction
FF	Fast Forwarding
FFA	Fast Forwarding Agent
ffAck	Fast Forward Acknowledgement
ffNAck	Fast Forward Negative Acknowledgement
ffNotify	Fast Forward Notify
FR	Festnetzrechner

GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HA	Home Agent
HSCSD	High Speed Circuit Switched Data
I-TCP	Indirekt TCP (Ansatz von Bakre et. al.)
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IOCTL	I/O Control
IP	Internet Protocol
IPsec	Secure IP
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IrDA	Infrared Data Association
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
LAN	Local Area Network
M-TCP	
M-TPI	M-Transportinstanz
MAC	Medium Access Control
METP	
MH	Mobile Host
MIG	Migration
MIP	Mobile IP
ms	Millisekunde
MS	Mobiles System
MTU	Maximum Transmission Unit
NMT	Nordic Mobile Telephone
OMIT	Optimierte Mobilitätsunterstützung für Indirekte Transportansätze
PAR	Positive Acknowledgment with Retransmission
PC	Personal Computer
PCB	Protocol Control Block
PDA	Personal Digital Assistent
PDU	Protocol Data Unit
QoS	Quality of Service
REQ	Request
RFC	Request For Comments
RLP	Radio Link Protocol

RTO	Retransmission Timeout (TCP)
RTT	Round Trip Time
s	Sekunde
SACK	Selective Acknowledgment
Seq	Sequenznummer
SNAP	Subnetwork Access Protocol
TCP	Transmission Control Protocol
TG	Transportgateway
TO	Timeout
TP	Transportprotokoll
TPCB	Transport Prococol Control Block
TPI	Transportinstanz
TTL	Time To Live
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network

Literaturverzeichnis

[ABSK95] E. Amir, H. Balakrishnan, S. Seshan und R. H. Katz: *Efficient TCP over Networks with Wireless Links.* Proceedings of Fifth Workshop of Hot Topics in Operating Systems, Orcas Island, WA, Mai 1995.

[AFH+99] B. Andersson, D. Forsberg, J. Hautio, J. Malinen, K. Mustonen und T. Weckström: *Dynamics - HUT Mobile IP.* Helsinki University of Technology, 1999. URL: http://www.cs.hut.fi/Research/Dynamics/.

[AKL+95] T. Alanko, M. Kojo, H. Laamanen, M. Liljeberg, M. Moilanen und K. Raatikainen: *Measured Performance of Data Transmission Over Cellular Telephone Networks.* Computer Communication Review, Vol. 24, no. 5, Oktober 1995.

[AKLR97] T. Alanko, M. Kojo, M. Liljeberg und K. Raatikainen: *Mowgli: Improvements for Internet Applications Using Slow Wireless Links.* Proceedings of 8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Helsinki, Finland, September 1997.

[All00] M. Allman: *A Web Server's View of the Transport Layer.* ACM Computer Communication Review, Oktober 2000.

[APS99] M. Allman, V. Paxson und W. Stevens: *TCP Congestion Control.* RFC 2581, April 1999.

[ARL97] *ARLAN Users Guide.* Aironet, http://www.aironet.com, 1997.

[Bak96] A. Bakre: *Design and Implementation of Indirect Protocols for Mobile Wireless Environments.* Dissertation at Rutgers, New Brunswick, the State University of New Jersey, Oktober 1996.

[BB95a] A. Bakre und B. R. Badrinath: *Handoff and System Support for Indirect TCP/IP.* Proceedings of the 2nd Usenix Symposium on Mobile and Location Independent Computing, April 1995.

[BB95b] A. Bakre und B. R. Badrinath: *I-TCP: Indirect TCP for Mobile Hosts.* Proceedings of 15th International Conf. on Distributed Computing Systems (ICDCS), Mai 1995.

[BBD+99] M. Beck, H. Böhme, M. Dziadzka, U. Kunitz, R. Magnus, C. Schröter und D. Verworrner: *Linux Kernelprogrammierung: Algorithmen und Strukturen , 5. Auflage.* Addison-Wesley Verlag, ISBN 3-8273-1476-3, 1999.

[BBIM93] B. R. Badrinath, A. Bakre, T. Imielinski und R. Marantz: *Handling Mobile Clients: A Case for Indirect Interaction.* Proceedings of the IEEE Fourth Workshop on Workstation Operating Systems, Oktober 1993.

[BBKT97] P. Bhagwat, P. Bhattacharya, A. Krishna und K. Tripathi: *Using channel state dependent packet scheduling to improve TCP throughput over wireless LANs.* Wireless Networks, vol. 3, no. 1, 1997.

[BBM97] M. Baker, J. Binkley und J. McHugh: *Secure Mobile Networking Project.* The Portland State University, 1997. URL: http://www.cs.pdx.edu/research/SMN/index.html.

[BHZ98] R. Bruyeron, B. Hemon und L. Zhang: *Experimentations with TCP Selective Acknowledgment.* ACM SIGCOMM, vol. 28, no. 2, April 1998.

[BKG+00] J. Border, M. Kojo, J. Griner, G. Montenegro und Z. Shelby: *Performance Enhancing Proxies.* Internet Draft: draft-ietf-pilc-pep-05.txt, November 2000.

[BKVP97] B. S. Bakshi, P. Krishna, N. H. Vaidya und D. K. Pradhan: *Improving Performance of TCP over Wireless Networks.* International Conference on Distributed Computing Systems, ICDCS'97, Baltimore, Mai 1997.

[BMJ+98] J. Broch, D. Maltz, D. Johnson, Y. Hu und J. Jetcheva: *Performance of Multi-Hop Wireless Ad Hoc Network Routing Protocols.* Proceedings of ACM/IEEE Mobicom'98, Dallas, USA, Oktober 1998.

[Bö96] A. Böger: *Migrationsunterstützung für Mobile Systeme.* Diplomarbeit, TU Braunschweig, 1996.

[Bro97] K. Brown: *Communication Protocols for Wireless Mobile Networks.* Dissertation at the University of South Carolina, 1997.

[BS97] K. Brown und S. Singh: *M-TCP: TCP for Mobile Cellular Networks.* Computer Communications Review, vol. 27 no. 5, Oktober 1997.

[BSAK95] H. Balakrishnan, S. Seshan, E. Amir und R. H. Katz: *Improving TCP/IP Performance over Wireless Networks.* Proceedings of Mobicom'95, Berkeley, California, November 1995.

[BSK95] H. Balakrishnan, S. Seshan und R. H. Katz: *Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks.* Wireless Networks, vol. 1, no. 4, Dezember 1995.

[BV98] S. Biaz und N. H. Vaidya: *Distinguishing Congestion Losses from Wireless Transmission Losses : A Negative Result.* Seventh International Conference on Computer Communications and Networks (IC3N), New Orleans, Oktober 1998.

[BW97] G. Brasche und B. Walke: *Concepts, Services, and Protocols of the New GSM Phase 2+ General Packet Radio Service.* IEEE Communications Magazine, vol. 35, no. 8, August 1997.

[BZCS96] M. G. Baker, X. Zhao, S. Cheshire und J. Stone: *Supporting Mobility in MosquitoNet.* USENIX Technical Conference, San Diego, CA, Januar 1996.

[CG97] J. Cai und D. J. Goodman: *General Packet Radio Service in GSM.* IEEE Communications Magazine, vol. 35, no. 10, Oktober 1997.

[Cho96] F. C. Choong: *Mobile IP at NUS.* National University of Singapore, 1996. URL: http://mip.ee.nus.edu.sg/.

[CI95] R. Caceres und L. Iftode: *Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments.* IEEE Journal on Selected Areas in Communications, vol. 13, no. 5, Juni 1995.

[CKV+99] A. Campbell, M. Kounavis, J. Vicente, M. Villela, K. Miki und H. De Meer: *A Survey of Programmable Networks.* SIGCOMM Computer Communication Review, April 1999.

[CL97] B. G. Chun und B. G. Lee: *Auxiliary Timeout and Selective Packet Discard Schemes to Improve TCP Performance in PCN Environment.* Proceedings of International Conference on Computers and Communications, ICC'97, Montreal, Canada, Juni 1997.

[CL98] M. C. Chuah und Y. Li: *Distributed Registration Extension to Mobile IP.* Internet Draft, Internet Engineering Task Force (IETF), draft-chuahli-mobileip-drempip.txt, November 1998.

[CRVP98] K. Chandran, S. Raghunathan, S. Venkatesan und R. Prakash: *A Feedback Based Scheme For Improving TCP Performance In Ad-Hoc Wireless Networks.* 18th International Conference on Distributed Computing Systems (ICDCS'98), Amsterdam, Netherlands, Mai 1998.

[Dar00] GMD-IPSI Darmstadt: *Überblick über Mobile IP Implementierungen (IPv4 und IPv6).* http://www.darmstadt.gmd.de/mobile/projects/miriam/implementation/index.html, 2000.

[DCY93] A. DeSimone, M. C. Chuah und O. C. Yue: *Throughput Performance of Transport-Layer Protocols over Wireless LANs.* Proceedings of Globecom '93, Dezember 1993.

[Dee91] S. Deering: *ICMP Router Discovery Messages.* RFC 1256, September 1991.

[Die98] J. Diederich: *Ressourcenreservierung für Mobile Systeme.* Diplomarbeit, TU Braunschweig, 1998.

[DPR00] S. Das, C. Perkins und E. Royer: *Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks.* Proceedings of IEEE Infocom'00, Tel-Aviv, Israel, März 2000.

[DR92] D. Duchamp und N. F. Reynolds: *Measured Performance of a Wireless LAN.* Proceedings of the 17th Converence on Local Computer Networks, 1992.

[Dro97] R. Droms: *Dynamic Host Configuration Protocol.* RFC 2131, März 1997.

[Dul00] W. Dulz: *WAP: Wireless Application Protocol.* Informatik Spektrum, Band 23, Heft 4, August 2000.

[EALSG95] S. Paul E. Ayanoglu, T. LaPorta, K. Sabnani und R. Gitlin: *Airmail: A link-layer protocol for wireless networks.* Wireless Networks, vol. 1, no. 1, 1995.

[ES96] D. A. Eckhardt und P. Steenkiste: *Measurement and Analysis of Error Characteristics of an In-Building Wireless Network.* Proceedings of the ACM SIGCOMM '96 Symposium, San Francisco, CA, August 1996.

[ES98a] D. A. Eckhardt und P. Steenkiste: *A Trace-based Evaluation of Adaptive Error Correction for a Wireless Local Area Network.* Mobile Networks and Applications, 1998.

[ES98b] D. A. Eckhardt und P. Steenkiste: *Improving Wireless LAN Performance via Adaptive Local Error Control.* Sixth IEEE International Conference on Network Protocols (ICNP'98) Austin, Oktober 1998.

[ETS97] *High Speed Circuit Switched Data (HSCSD) - Stage 1, GSM specification 02.34.* European Telecommunications Standards Institute (ETSI), April 1997.

[EV97] J. Eberspächer und H. J. Vögel: *GSM, Global System for Mobile Communication.* Teubner Verlag Stuttgart, ISBN 3-51906192-9, 1997.

[FBZ97] A. Fieger, A. Böger und M. Zitterbart: *Migrating State Information in Mobile Environments.* Fifth IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS'97), Tunis, Tunisia, Oktober 1997.

[FC98] S. F. Foo und K. C. Chua: *Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs.* draft-chuafoo-mobileip-rafa-00.txt, November 1998.

[FDZ99] A. Fieger, J. Diederich und M. Zitterbart: *Optimierung von Subnetzwechseln mit Mobile IP.* Tagungsband; Kommunikation in verteilten Systemen (KiVS) 1999, Darmstadt, Germany, März 1999.

[FHMR98] C. Fan, B. Henckel, M. Mateescu und R. Ruppelt: *Interoperability Analysis and TCP Performance in a Heterogeneous Mobile-IP Environment.* 9th IEEE Workshop on Local and Metropolitan Area Networks, Banff, Canada, Mai 1998.

[FLM98] John Floroiu, Thomas Luckenbach und Mihai Mateescu: *Mobile IP on Windows NT.* GMD Fokus, Berlin, University of Bucharest, http://mip-nt.aii.pub.ro/, 1998.

[Flo94] S. Floyd: *TCP and Explicite Congestion Notification.* Computer Communication Review, vol. 24, no. 5, Oktober 1994.

[FRSW98] F. H. P. Fitzek, B. Rathke, M. Schläger und A. Wolisz: *Simultaneous MAC-Packet Transmission in Integrated Broadband Mobile System for TCP.* Proceedings of ACTS SUMMIT 1998, Juni 1998.

[FS98] P. Ferguson und D. Senie: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.* RFC 2267, Januar 1998.

[FS99] A. Fladenmuller und R. De Silva: *The effect of Mobile IP handoffs on the performance of TCP.* Mobile Networks and Applications, vol. 4, no. 2, Mai 1999.

[FZ96] A. Fieger und M. Zitterbart: *Wireless Local Area Networks.* Technical Report (82 pages), TU Braunschweig, ZFE Siemens (Munich), November 1996.

[FZ97a] A. Fieger und M. Zitterbart: *Evaluation of Migration Support for Indirect Transport Protocols.* 2nd Global Internet Conference in conjunction with Globecom'97, Phoenix, Arizona, USA, November 1997.

[FZ97b] A. Fieger und M. Zitterbart: *Migration Support for Indirect Transport Protocols.* Proceedings of International Conference on Universal Personal Communications '97, San Diego, California, USA, Oktober 1997.

[FZ97c] A. Fieger und M. Zitterbart: *Transport Protocols over Wireless Links.* Proceedings of 2nd IEEE Symposium on Computer and Communications (ISCC'97), Alexandria, Egypt, Juli 1997.

[FZKD99] A. Fieger, M. Zitterbart, R. Keller und J. Diederich: *Towards QoS-support in the Presence of Handover.* Proceedings of First Workshop on IP Quality of Service for Wireless and Mobile Networks (IQWiM'99), April 1999.

[GCW98] M. Gerla, R. L Cigno und W. Weng: *Improving wireless handoff with GWA-TCP.* Technical Report No. 990021, UCLA, University of California, Los Angeles, 1998.

[GD96] V. Gupta und A. Dixit: *Mobile IP for Linux (ver. 1.00).* Dept. of Computer Science, State University of New York, Binghamton, 1996. URL: http://anchor.cs.binghamton.edu/~mobileip/.

[GJP00] E. Gustafsson, A. Jonsson und C. E. Perkins: *Mobile IP Regional Registration.* Internet Draft, Internet Engineering Task Force (IETF), draft-ietf-mobileip-reg-tunnel-02.txt, März 2000.

[GMPG00] T. Goff, J. Moronski, D. Phatak und V. Gupta: *Freeze-TCP: A true end-to-end TCP enhancement mechanism for mobile environments.* Proceedings of IEEE Infocom'00, Tel-Aviv, Israel, März 2000.

[Gup98] V. Gupta: *Solaris Mobile IP: Design and Implementation.* http://playground.sun.com/pub/mobile-ip/SolarisMobileIP.ps, Februar 1998.

[HA97] Z. J. Haas und P. Agrawal: *Mobile-TCP: An Asymmetric Transport Protocol Design for Mobile Systems.* Proceedings of International Conference on Computers and Communications, ICC'97, Montreal, Canada, Juni 1997.

[Hal96] Fred Halsall: *Data Communications, Computer Networks and Open Systems.* Addison-Wesley, ISBN 0-201-42293-X, 1996.

[HLFT94] S. Hanks, T. Li, D. Farinacci und P. Traina: *Generic Routing Encapsulation (GRE).* RFC 1701, Oktober 1994.

[HNI+98] J. Haartsen, M. Naghshineh, J. Inouye, O. Joeressen und W. Allen: *Bluetooth: Vision, Goals, and Architecture*, Oktober 1998.

[Hui00] C. Huitema: *Routing in the Internet (second Edition).* Prentice Hall, ISBN: 0-13-0022647-5, 2000.

[HWB00] J. Huber, D. Weiler und H. Brand: *UMTS, the Mobile Multimedia Vision for IMT-2000: A Focus on Standardization.* IEEE Communications Magazine, vol. 38, no. 9, September 2000.

[IDJ92] J. Ioannidis, D. Duchamp und G. Q. Maquire Jr.: *Protocols for Mobile Internetworking.* Draft RFC, Juni 1992.

[IEE99] *IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.* IEEE Standard, 1999.

[Jac90] V. Jacobson: *Compressing TCP/IP headers for Low-Speed Serial Links.* RFC 1144, Februar 1990.

[JBB92] V. Jacobson, R. Braden und D. Borman: *TCP Extensions for High Performance.* RFC 1323, Mai 1992.

[JK98] V. Jacobson und M. J. Karels: *Congestion Avoidance and Control.* Proceedings of ACM SIGCOMM, 1998.

[JP00] D. Johnson und C. Perkins: *Mobility Support in IPv6.* Internet Draft, Internet Engineering Task Force, draft-ietf-mobileip-ipv6-13.txt, November 2000.

[KA98] S. Kent und R. Atkinson: *Security Architecture for the Internet Protocol.* RFC 2401, November 1998.

[KP87] P. Karn und C. Partridge: *Estimating Round-Trip Times in Reliable Transport Protocols.* Proc. SIGCOMM '87, August 1987.

[KRL+97] M. Kojo, K. Raatikainen, M. Liljeberg, J. Kiiskinen und T. Alanko: *An Efficient Transport Service for Slow Wireless Telephone Links.* IEEE Journal on Selected Areas in Communications, vol. 15, no. 7, September 1997.

[LK00] R. Ludwig und R. H. Katz: *The Eifel Algorithm: Making TCP Robust against Spurious Retransmissions.* Computer Communication Review, ACM SIGCOMM, vol. 30, no. 1, Januar 2000.

[LKJK99] R. Ludwig, A. Konrad, A. D. Joseph und R. H. Katz: *Optimizing the End-to-End Performance of Reliable Flows over Wireless Links.* Proceedings of ACM/IEEE Mobicom'99, Seattle, USA, August 1999.

[LRK+99] R. Ludwig, B. Rathonyi, A. Konrad, K. Oden und A. Joseph: *Multilayer Tracing of TCP over Reliable Wireless Link.* Proceedings of ACM SIGMETRICS 1999, 1999.

[LS98] P. Lettieri und M. B. Srivastava: *Adaptive Frame Length Control for Improving Wireless Link Throughput, Range, and Energy Efficiency.* Proceedings of IEEE Infocom'98, San Francisco, CA, USA, April 1998.

[LS00] R. Ludwig und K. Sklower: *The Eifel Retransmission Timer.* ACM Computer Communications Review, vol. 30, no. 3, Juli 2000.

[Lud99] R. Ludwig: *A Case for Flow-Adaptive Wireless Links.* Technical Report UCB//CSD-99-1053, University of California Berkeley, Mai 1999.

[Lud00] R. Ludwig: *Eliminating Inefficient Cross-Layer Interactions in Wireless Networking.* Dissertation an der RWTH Aachen, April 2000.

[Mad97] W. Mader: *Erstellung eines Visualisierungstools für die Simulationsumgebung SimPlusPlus.* Studienarbeit, TU Braunschweig, 1997.

[MB98] D. A. Maltz und P. Bhagwat: *MSOCKS: An Architecture for Transport Layer Mobility.* Proceedings of IEEE Infocom'98, San Francisco, CA, USA, April 1998.

[MHW+99] P. McCann, T. Hiller, J. Wang, A. Casati, C. E. Perkins und P. Calhoun: *Transparent Hierachical Mobility Agents (THEMA).* draft-mccann-thema-00.txt, März 1999.

[MHWZ99] B. Metzler, T. Harbaum, R. Wittmann und M. Zitterbart: *AMnet: Heterogeneous Multicast Services based on Active Networking.* Proc. of the 2nd Workshop on Open Architectures and Network Programming (OPENARCH99), New York, USA, März 1999.

[MJ97] D. Maltz und D. Johnson: *IETF Mobile IPv4 for 4.4BSD-based Unix systems.* Carnegie Mellon University, Computer Science Departement, 1997. URL: http://www.monarch.cs.cmu.edu/.

[MMFR96] M. Mathis, J. Mahdavi, S. Floyd und A. Romanow: *TCP Selective Acknowledgment Options.* IETF, RFC 2018, Oktober 1996.

[Mon01] C. Montenegro: *Reverse Tunneling for Mobile IP, revised.* RFC 3024, Januar 2001.

[MP92] M. Mouly und M. B. Pautet: *The Global System for Mobile (GSM) Communications.* Cell and SYS Press, ISBN 2-9507190-0-7, 1992.

[PCM98] *PCMCIA Package mit WaveLAN Treibern, Version 3.0.6*, November 1998.

[Per96a] C. Perkins: *IP Encapsulation within IP.* RFC 2003, Oktober 1996.

[Per96b] C. Perkins: *IP Mobility Support.* RFC 2002, Oktober 1996.

[Per96c] C. Perkins: *Minimal Encapsulation within IP.* RFC 2004, Oktober 1996.

[Per96d] C. Perkins: *Mobile-IP Local Registration with Hierarchical Foreign Agents.* draft-perkins-mobileip-hierfa-00.txt, Februar 1996.

[Per98a] C. Perkins: *Mobile IP, Design Principles and Practices.* Addison-Wesley Publishing Company, ISBN 0-201-63469-4, Januar 1998.

[Per98b] C. Perkins: *Mobile Networking through Mobile IP.* IEEE Internet computing, Januar 1998.

[PGLA99] C. Parsa und J. J. Garcia-Lunz-Aceves: *Improving TCP Congestion Control over Internets with Heterogeneous Transmission Media.* Seventh Annual International Conference on Network Protocols, ICNP'99, Toronto, Canada, Oktober 1999.

[PGLA00] C. Parsa und J. J. Garcia-Luna-Aceves: *Improving TCP Performance over Wireless Networks at the Link Layer.* ACM Mobile Networks and Applications Journal, April 2000.

[PJ95] C. Perkins und T. Jagannadh: *DHCP for Mobile Networking with TCP/IP.* IEEE Symposium on Computers and Communications, Alexandria, Egypt, Juni 1995.

[PJ00] C. Perkins und D. Johnson: *Route Optimization in Mobile IP.* Internet Draft, Internet Engineering Task Force, draft-ietf-mobileip-optim-10.txt, November 2000.

[Pos84] J. Postel: *Multi-LAN Address Resolution.* RFC 925, Oktober 1984.

[RF99] K. Ramakrishnan und S. Floyd: *A Proposal to add Explicit Congestion Notification (ECN) to IP.* RFC 2481, Januar 1999.

[RL93] Y. Rekhter und T. Li: *An Architecture for IP Address Allocation with CIDR.* RFC 1518, September 1993.

[RL94] Y. Rekhter und T. Li: *A Border Gateway Protocol 4 (BGP-4).* RFC 1518, July 1994.

[Ros92a] O. Rose: *Sim PlusPlus: An object-oriented language for process-oriented discret-event simulation.* Interner Bericht 31/1992, Institut für Telematik, Universität Karlsruhe, 1992.

[Ros92b] O. Rose: *Sim PlusPlus: Part II - SimEnv: An object-oriented simulation-environment for network analysis.* Interner Bericht 31/1992, Institut für Telematik, Universität Karlsruhe, 1992.

[RSW98] B. Rathke, M. Schläger und A. Wolisz: *Systematic Measurement of TCP Performance over Wireless LANs.* Technical Report TKN-01BR98, Technical University of Berlin, Department of Electrical Engineering, Dezember 1998.

[RT99] E. Royer und C. H. Toh: *A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks.* IEEE Personal Communications, April 1999.

[SB00] A. C. Snoeren und H. Balakrishnan: *TCP Connection Migration.* Internet Draft: draft-snoeren-tcp-migrate-00.txt, November 2000.

[SBK97] S. Seshan, H. Balakrishnan und R. H. Katz: *Handoffs in Cellular Wireless Networks: The Daedalus Implementation and Experience*, März 1997. URL: http://www-daedalus.cs.berkeley.edu/publications/kluwer.ps.gz.

[SC+00] H. Soliman, C. Castelluccia, , K. El-Malki und L. Bellier: *Hierarchical MIPv6 mobility management*. Internet Draft, Internet Engineering Task Force, draft-ietf-mobileip-hmipv6-01.txt, September 2000.

[Sch00] M. Schläger: *The TCP Eifel-Algorithm for Linux*. http://www-tkn.ee.tu-berlin.de/~morten/eifel, Juli 2000.

[Ses95] S. Seshan: *Low-Latency Handoff for Cellular Data Networks*. Dissertation at the University of California Berkeley, USA, 1995.

[SF98] N. K. Samaraweera und G. Faerhurst: *Reinforcement of TCP Error Recovery for Wireless Communications*. ACM SIGCOMM, Computer Communication Review, vol. 28, no. 2, April 1998.

[SMA98] J. M. Sicilia und J. Miguel-Alonso: *An architecture to access data services through cellular phone networks*. Euromicro Summer School on Mobile Computing '98, Oulu, Finnland, August 1998.

[SRBW00] M. Schläger, B. Rathke, S. Bodenstein und A. Wolisz: *Advocating a Remote Socket Architecture for Internet Access using Wireless LANs*. MONET: Special Issue on Wireless Internet and Intranet Access, 2000.

[Ste94] W. R. Stevens: *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley, ISBN 0-201-63346-9, 1994.

[Str99] T. Ströhlein: *Simulative Untersuchung von Migrationsstrategien für mobile Systeme*. Diplomarbeit, TU Braunschweig, 1999.

[SZD96] A. Schill, T. Ziegert und N. Diehl: *Mobile IP: Überblick und Systemvergleich*. PIK, Praxis der Informationsverarbeitung und Kommunikation, 1996.

[TMW97] K. Thompsons, G. J. Miller und R. Wilder: *Wide-Area Internet Traffic Patterns and Characteristics*. IEEE Network Magazine, vol. 11 no. 6, Dezember 1997.

[TSS+97] D. L. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall und G. J. Minden.: *A Survey of Active Network Research*. ICM, 35(1):80–86, Januar 1997.

[VMPM99] N. Vaidya, M. Mehta, C. E. Perkins und G. Montenegro: *Delayed Duplicate Acknowledgements: A TCP-Unaware Approach to Improve Performance of TCP over Wireless*. Technical Report 99-003, Texas A&M University, URL: http://www.cs.tamu.edu/faculty/vaidya/Vaidya-mobile.html, Februar 1999.

[Wav96] *WaveLAN/PCMCIA Card, Users Guide*. Lucent Technologies, Bell Labs Innovations, Oktober 1996.

[Wav97] *WaveLAN Air Interface Data Manual.* Lucent Technologies, Bell Labs Innovations, April 1997.

[Wav99] *WaveLAN IEEE 802.11, Users Guide.* Lucent Technologies, Bell Labs Innovations, 1999.

[Wol99] A. Wolisz: *Mobility in Multimedia Communication.* Beitrag im Tagungsband vom 2. WAKI/G-IIA-Symposium: Verteilte multimediale Anwendungen und diensteintegrierende Kommunikationsnetze, 1999.

[WS95] G. R. Wright und W. R. Stevens: *TCP/IP Illustrated, Volume 2: The Implementation.* Addison-Wesley, ISBN 0-201-63354-X, 1995.

[WT98] K. Y. Wang und S. K. Tripathi: *Mobile-End Transport Protocols: An Alternative to TCP/IP over Wireless Links.* Proceedings of IEEE Infocom'98, San Francisco, CA, USA, April 1998.

[YB94] R. Yavatkar und N. Bhagawat: *Improving End-to-End Performance of TCP over Mobile Internetworks.* IEEE Workshop on Mobile Computing, Dezember 1994.

[ZF96] M. Zitterbart und A. Fieger: *End-to-End communications across hybrid networks.* W. Effelsberg, O. Spaniol, A. Danthine, D. Ferrari (Eds.), High-Speed Networking for Multimedia Applications, Kluwer-Academic Publishers, Januar 1996.

[ZR97] M. Zorzi und R. R. Rao: *The Role of Error Correlations in the Design of Protocols for Packet Switched Services.* 35th Annual Conference on Communication, Control and Computing, Monticello, IL, USA, Oktober 1997.

[ZS00] Y. Zhang und B. Singh: *A Multi-Layer IPsec Protocol.* Proceedings of 9th USENIX Security Symposium, Denver, Colorado, August 2000.

Index